NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
5.1	Organisation of Information Security (OIS)	Objective: Plan, implement, maintain and continuously improve the information security framework within the organisation.	Functional	No Relationship	N/A	N/A	N/A	0		
OIS-01.01B	Information Security Management System (ISMS)	The cloud service provider maintains an ISO/IEC 27001-compliant information security management system (ISMS). The scope of the ISMS covers the cloud service provider's organisational units, locations, zones, regions and procedures relevant to the development and operation of the cloud service.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	8		GOV-01
OIS-01.01B	Information Security Management System (ISMS)	The cloud service provider maintains an ISO/IEC 27001-compliant information security management system (ISMS). The scope of the ISMS covers the cloud service provider's organisational units, locations, zones, regions and procedures relevant to the development and operation of the cloud service.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure	5		GOV-01.4
OIS-01.02B	Information Security Management System (ISMS)	The measures for setting up, implementing, maintaining and continuously improving the ISMS are documented. The documentation includes:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
OIS-01.02B	Information Security Management System (ISMS)	The measures for setting up, implementing, maintaining and continuously improving the ISMS are documented. The documentation includes:	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		IAO-03
OIS-01.02B.1	Information Security Management System (ISMS)	Context of the cloud service provider;	Functional	Intersects With	Defining Business Context & Mission	GOV-06	Mechanisms exist to document the organization's business model and mission.	5		GOV-08
OIS-01.02B.2	Information Security Management System (ISMS)	Scope of the ISMS (section 4.3 of ISO/IEC 27001);	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		IAO-03
OIS-01.02B.3	Information Security Management System (ISMS)	Statement of applicability (section 6.1.3 of ISO/IEC 27001);	Functional	Intersects With	Select Controls	GOV-11.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15.1
OIS-01.02B.4	Information Security Management System (ISMS)	Overview of how activities in the ISMS cover the cloud service;	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	3		GOV-01
OIS-01.02B.5	Information Security Management System (ISMS)	Description of how the cloud service provider maintains and improves the cloud service's security; and	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and	5		GOV-03
OIS-01.02B.6	Information Security Management System (ISMS)	Results of the last management review (section 9.3 of ISO/IEC 27001).	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2
OIS-01.03B	Information Security Management System (ISMS)	Additionally, the cloud service provider documents the scope and boundaries of the cloud service under its operational control, including any exclusions or shared-responsibility areas.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	5		CLD-06.1
OIS-01.03B	Information Security Management System (ISMS)	Additionally, the cloud service provider documents the scope and boundaries of the cloud service under its operational control, including any exclusions or shared-responsibility areas.	Functional	Intersects With	Compliance Scope	CPL-03	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance	5		CPL-01.2
OIS-01.03B	Information Security Management System (ISMS)	Additionally, the cloud service provider documents the scope and boundaries of the cloud service under its operational control, including any exclusions or shared-responsibility areas.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5		IAO-03
OIS-01.01AS	Information Security Management System (ISMS)	OIS-01.01AS, sharpening OIS-01.01B The Information Security Management System (ISMS) has a valid certification according to ISO/IEC 27001 or ISO 27001 based on BSI IT-Grundschutz. The scope of the certification covers the cloud service provider's organisational units, locations, zones, regions, and procedures relevant to the development and operation of the cloud service.	Functional	Intersects With	Compliance Scope	CPL-03	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5		CPL-01.2
OIS-01.01AS	Information Security Management System (ISMS)	OIS-01.01AS, sharpening OIS-01.01B The Information Security Management System (ISMS) has a valid certification according to ISO/IEC 27001 or ISO 27001 based on BSI IT-Grundschutz. The scope of the certification covers the cloud service provider's organisational units, locations, zones, regions, and procedures relevant to the development and operation of the cloud service.	Functional	Intersects With	Statement of Applicability (SOA)	CPL-25	Mechanisms exist to produce a Statement of Applicability (SOA), or similar document, for compliance-related scoping activities.	5		CPL-12
OIS-01.01AS	Information Security Management System (ISMS)	OIS-01.01AS, sharpening OIS-01.01B The Information Security Management System (ISMS) has a valid certification according to ISO/IEC 27001 or ISO 27001 based on BSI IT-Grundschutz. The scope of the certification covers the cloud service provider's organisational units, locations, zones, regions, and procedures relevant to the development and operation of the cloud service.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure practices.	3		GOV-01.4
OIS-01.01AS	Information Security Management System (ISMS)	OIS-01.01AS, sharpening OIS-01.01B The Information Security Management System (ISMS) has a valid certification according to ISO/IEC 27001 or ISO 27001 based on BSI IT-Grundschutz. The scope of the certification covers the cloud service provider's organisational units, locations, zones, regions, and procedures relevant to the development and operation of the cloud service.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	8		TPM-05.8

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OIS-01.01AC	Information Security Management System (ISMS)	Existing valid certifications according to ISO/IEC 27001 are issued and recognised by an accredited certification body.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	8		TPM-05.8
OIS-02.01B	Information Security Policy	Top management of the cloud service provider has adopted an information security policy.	Functional	Intersects With	Security, Compliance & Resilience Governance Policy	GOV-01	Mechanisms exist to establish a formal, documented security, compliance and resilience governance policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving risks, threats and other changes that affect the organization.	8		
OIS-02.01B	Information Security Policy	Top management of the cloud service provider has adopted an information security policy.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10		GOV-02
OIS-02.02B	Information Security Policy	Top management of the cloud service provider has communicated the information security policy to internal and external personnel as well as cloud service customers.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8		GOV-02
OIS-02.03B	Information Security Policy	The information security policy describes:	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10		GOV-02
OIS-02.03B.1	Information Security Policy	The importance of information security, based on the requirements of cloud service customers in relation to information security;	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10		GOV-02
OIS-02.03B.2	Information Security Policy	The security objectives and the desired security level, based on the business goals and activities as well as compliance obligations of the cloud service provider;	Functional	Intersects With	Control Objectives	GOV-03.3	Mechanisms exist to establish control objectives as the basis for the design, selection, implementation and management of the organization's internal security, compliance and resilience control system.	5		GOV-09
OIS-02.03B.3	Information Security Policy	The cloud service provider's commitment to implement the necessary security measures for fulfilling the established security objectives;	Functional	Intersects With	Business As Usual (BAU) Security, Compliance & Resilience Practices	GOV-10	Mechanisms exist to incorporate security, compliance and resilience principles into Business As Usual (BAU) practices through executive leadership involvement.	8		PRM-01
OIS-02.03B.3	Information Security Policy	The cloud service provider's commitment to implement the necessary security measures for fulfilling the established security objectives;	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-04	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	8		GOV-14
OIS-02.03B.4	Information Security Policy	The most important aspects of the security strategy to achieve the security objectives set; and	Functional	Intersects With	Strategic Plan & Objectives	PRM-02	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5		PRM-01.1
OIS-02.03B.5	Information Security Policy	The organisational structure for information security in the scope of the ISMS.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5		GOV-04
OIS-02.03B.5	Information Security Policy	The organisational structure for information security in the scope of the ISMS.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
OIS-03.01B	Interfaces and Dependencies	The cloud service provider establishes, documents, and communicates a Shared Security Responsibility Model (SSRM) to define and manage interfaces and dependencies between cloud service delivery activities performed by the cloud service provider and those performed by cloud service customers.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	8		CLD-06.1
OIS-03.02B	Interfaces and Dependencies	The SSRM documentation clearly defines the responsibilities between both parties for handling vulnerabilities, security incidents, and incidents. The type and scope of the documentation is geared towards the information requirements of the subject matter experts of the affected organisations in order to carry out the activities appropriately (e.g. definition of roles and responsibilities in guidelines, description of cooperation obligations in service descriptions and contracts).	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	5		CLD-06.1
OIS-03.02B	Interfaces and Dependencies	The SSRM documentation clearly defines the responsibilities between both parties for handling vulnerabilities, security incidents, and incidents. The type and scope of the documentation is geared towards the information requirements of the subject matter experts of the affected organisations in order to carry out the activities appropriately (e.g. definition of roles and responsibilities in guidelines, description of cooperation obligations in service descriptions and contracts).	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-11	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5		TPM-05.4
OIS-03.03B	Interfaces and Dependencies	The cloud service provider regularly reviews and validates the SSRM documentation in accordance with SP-02 to ensure its accuracy and relevance for all cloud service offerings.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	5		CLD-06.1
OIS-03.03B	Interfaces and Dependencies	The cloud service provider regularly reviews and validates the SSRM documentation in accordance with SP-02 to ensure its accuracy and relevance for all cloud service offerings.	Functional	Intersects With	Third-Party Scope Review	TPM-16	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure security, compliance and resilience control assignments accurately reflect current: (1) Contractual obligations for the External Service Provider (ESP); (2) Business practices; (3) Applicable stakeholders; and (4) Deployed Technology Assets, Applications and/or	5		TPM-05.5
OIS-03.04B	Interfaces and Dependencies	The cloud service provider implements, operates, and reviews the SSRM components for which it is responsible, ensuring adherence to the defined security measures.	Functional	Intersects With	Conformity Monitoring	CPL-05	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	3		CPL-03
OIS-03.04B	Interfaces and Dependencies	The cloud service provider implements, operates, and reviews the SSRM components for which it is responsible, ensuring adherence to the defined security measures.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-11	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15
OIS-03.05B	Interfaces and Dependencies	The communication of changes to the SSRM, interfaces and dependencies takes place in a timely manner so that the affected organisations and third parties can react appropriately with organisational and technical measures before the changes take effect.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		CHG-05
OIS-04.01B	Segregation of Duties	Conflicting tasks and responsibilities are segregated based on a risk assessment in accordance with OIS-07 to reduce the risk of unauthorised or unintended changes or misuse of cloud service customer data, cloud service derived data and cloud service provider data. The risk assessment covers the following areas, insofar as these are applicable to the provision of the cloud service and are in the area of responsibility of the cloud service provider:	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	8		HRS-11

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OIS-04.01B	Segregation of Duties	Conflicting tasks and responsibilities are segregated based on a risk assessment in accordance with OIS-07 to reduce the risk of unauthorised or unintended changes or misuse of cloud service customer data, cloud service derived data and cloud service provider data. The risk assessment covers the following areas, insofar as these are applicable to the provision of the cloud service and are in the area of responsibility of the cloud service provider:	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
OIS-04.01B.1	Segregation of Duties	Administration of a role, rights and authorisation framework based on role-based access control and the business and security requirements of the cloud service provider (cf. IAM-01);	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5		IAC-08
OIS-04.01B.2	Segregation of Duties	Development, testing and release of changes (cf. DEV-01);	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	3		CHG-01
OIS-04.01B.2	Segregation of Duties	Development, testing and release of changes (cf. DEV-01);	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	3		HRS-11
OIS-04.01B.3	Segregation of Duties	Risk management (cf. OIS-07); and	Functional	Intersects With	Position Categorization	HRS-03	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	3		HRS-02
OIS-04.01B.3	Segregation of Duties	Risk management (cf. OIS-07); and	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	3		HRS-11
OIS-04.01B.3	Segregation of Duties	Risk management (cf. OIS-07); and	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	3		RSK-01
OIS-04.01B.4	Segregation of Duties	Operation of the system components.	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	3		HRS-11
OIS-04.02B	Segregation of Duties	Mitigating measures are outlined in the risk treatment plan (cf. OIS-09) and implemented by the cloud service provider in a way that prioritises the segregation of duties.	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	3		HRS-11
OIS-04.02B	Segregation of Duties	Mitigating measures are outlined in the risk treatment plan (cf. OIS-09) and implemented by the cloud service provider in a way that prioritises the segregation of duties.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-17.1	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5		RSK-06.4
OIS-04.03B	Segregation of Duties	If segregation of duties cannot be implemented due to organisational or technical constraints, the cloud service provider establishes and operates compensating controls to monitor relevant activities. These controls are designed to detect unauthorised or unintended changes, misuse of data, or violations of operational policies, and enable timely and appropriate response actions.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
OIS-04.03B	Segregation of Duties	If segregation of duties cannot be implemented due to organisational or technical constraints, the cloud service provider establishes and operates compensating controls to monitor relevant activities. These controls are designed to detect unauthorised or unintended changes, misuse of data, or violations of operational policies, and enable timely and appropriate response actions.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	8		RSK-06.2
OIS-04.04B	Segregation of Duties	An inventory consisting of conflicting tasks, responsibilities and resolving measures is established and maintained by the cloud service provider. For the assignment, change or revocation of roles, rights and authorities, the cloud service provider enforces the segregation of duties.	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5		HRS-11
OIS-04.04B	Segregation of Duties	An inventory consisting of conflicting tasks, responsibilities and resolving measures is established and maintained by the cloud service provider. For the assignment, change or revocation of roles, rights and authorities, the cloud service provider enforces the segregation of duties.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	3		IAC-08
OIS-04.01AC	Segregation of Duties	To resolve conflicting roles, measures associated with the segregation of duties are monitored and enforced by the cloud service provider.	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5		HRS-11
OIS-04.01AC	Segregation of Duties	To resolve conflicting roles, measures associated with the segregation of duties are monitored and enforced by the cloud service provider.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
OIS-04.02AC	Segregation of Duties	Timely and appropriate remediation measures address any deviations identified during monitoring.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
OIS-05.01B	Threat Intelligence	The cloud service provider collects information from selected internal and external sources to gain a comprehensive view of the threat landscape that lead to cybersecurity risks.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5		THR-01
OIS-05.01B	Threat Intelligence	The cloud service provider collects information from selected internal and external sources to gain a comprehensive view of the threat landscape that lead to cybersecurity risks.	Functional	Intersects With	Threat Intelligence Feeds	THR-04	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	8		THR-03
OIS-05.02B	Threat Intelligence	The collected information is correlated and analysed to identify its potential impact on the cloud service provider's organisation.	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	8		THR-10
OIS-05.03B	Threat Intelligence	The cloud service provider integrates threat intelligence insights into its risk management process (cf. OIS-07, OIS-08 and OIS-09).	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	5		RSK-03
OIS-05.03B	Threat Intelligence	The cloud service provider integrates threat intelligence insights into its risk management process (cf. OIS-07, OIS-08 and OIS-09).	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5		THR-01
OIS-06.01B	Contact with Relevant Government Agencies and Interest Groups	If the cloud service is used by public sector organisations in Germany, the cloud service provider establishes and maintains contacts with the National IT Situation Centre and the CERT Association of the BSI as appropriate.	Functional	Intersects With	Contacts With Authorities	GOV-15	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	8		GOV-06

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OIS-07.01B	Risk Management Policy	Policies and procedures for risk management procedures are documented, communicated and provided in accordance with SP-01. Risk management procedures are based on a methodology for risk assessments. The methodology allows comparability and reproducibility for the following aspects:	Functional	Subset Of	Risk Management Policy	RSK-01	Mechanisms exist to establish a formal, documented risk management policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving	10		
OIS-07.01B	Risk Management Policy	Policies and procedures for risk management procedures are documented, communicated and provided in accordance with SP-01. Risk management procedures are based on a methodology for risk assessments. The methodology allows comparability and reproducibility for the following aspects:	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	8		RSK-01
OIS-07.01B	Risk Management Policy	Policies and procedures for risk management procedures are documented, communicated and provided in accordance with SP-01. Risk management procedures are based on a methodology for risk assessments. The methodology allows comparability and reproducibility for the following aspects:	Functional	Intersects With	Risk Assessment Methodology	RSK-12	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	5		RSK-04.2
OIS-07.01B.1	Risk Management Policy	Identification of cybersecurity risks and other risks associated with the loss of confidentiality, integrity, availability and authenticity of information within the scope of the ISMS and assigning risk owners;	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	5		RSK-03
OIS-07.01B.2	Risk Management Policy	Analysis of the probability and impact of occurrence and determination of the level of risk;	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04
OIS-07.01B.3	Risk Management Policy	Evaluation of the risk assessment based on defined criteria for risk acceptance and prioritisation of risk management;	Functional	Intersects With	Risk Tolerance	RSK-05.1	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5		RSK-01.3
OIS-07.01B.4	Risk Management Policy	Treatment of risks through measures, including approval of authorisation and acceptance of residual risks by risk owners;	Functional	Intersects With	Risk Treatment Options	RSK-16.1	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance and service provider); or (4) Accepting the risk.	5		RSK-06.3
OIS-07.01B.5	Risk Management Policy	Documentation of the activities implemented to enable consistent, valid and comparable results; and	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5		RSK-04.1
OIS-07.01B.6	Risk Management Policy	Evaluation of the risk assessment and the status of risk treatment plans by the level of management responsible for the security of the cloud service.	Functional	Intersects With	Risk Assessment Stakeholder Involvement	RSK-13.3	Mechanisms exist to: (1) Define applicable stakeholders for each risk assessment; (2) Involve identified stakeholders in the risk assessment process; and (3) Provide identified stakeholders with results of the risk assessment, upon completion.	5		RSK-04.4
OIS-08.01B	Application of the Risk Management Policy - Risk Assessment	The cloud service provider performs the risk management process specified by OIS-07 as needed and at least annually.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8		RSK-04
OIS-08.02B	Application of the Risk Management Policy - Risk Assessment	The following aspects are taken into account when identifying risks, insofar as they are applicable to the cloud service provided and are within the area of responsibility of the cloud service provider:	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	5		RSK-03
OIS-08.02B.1	Application of the Risk Management Policy - Risk Assessment	Processing, storage or transmission of cloud service customer data and cloud service derived data with different protection needs;	Functional	Intersects With	Risk-Based Security Categorization	RSK-07	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5		RSK-02
OIS-08.02B.2	Application of the Risk Management Policy - Risk Assessment	Occurrence of vulnerabilities and incidents in technical protective measures for separating shared resources;	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5		CLD-06
OIS-08.02B.3	Application of the Risk Management Policy - Risk Assessment	Attacks via access points, including interfaces accessible from public networks and accidentally exposed interfaces;	Functional	Intersects With	Attack Surface Scope	VPM-03	Mechanisms exist to define and manage the scope for its attack surface management activities.	3		VPM-01.1
OIS-08.02B.4	Application of the Risk Management Policy - Risk Assessment	Dependencies on service organisations;	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1
OIS-08.02B.5	Application of the Risk Management Policy - Risk Assessment	An encryption and key management risk programme which addresses the risks of unauthorised disclosure, modification, destruction, or information loss of cryptographic keys; and	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic	5		CRY-01
OIS-08.02B.6	Application of the Risk Management Policy - Risk Assessment	Separation of cloud service customers and their data within systems, networks and storage.	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5		CLD-06
OIS-08.03B	Application of the Risk Management Policy - Risk Assessment	Policies and procedures covering risk assessments relevant for the delivery and operation of the cloud service are implemented by the cloud service provider.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5		RSK-01
OIS-08.04B	Application of the Risk Management Policy - Risk Assessment	The risk assessment's results are provided to relevant internal parties.	Functional	Intersects With	Risk Assessment Stakeholder Involvement	RSK-13.3	Mechanisms exist to: (1) Define applicable stakeholders for each risk assessment; (2) Involve identified stakeholders in the risk assessment process; and (3) Provide identified stakeholders with results of the risk assessment, upon completion.	5		RSK-04.4
OIS-08.05B	Application of the Risk Management Policy - Risk Assessment	Relevant external parties are provided with information, specific to the parties' purposes, resulting from the risk assessments.	Functional	Intersects With	Risk Assessment Stakeholder Involvement	RSK-13.3	Mechanisms exist to: (1) Define applicable stakeholders for each risk assessment; (2) Involve identified stakeholders in the risk assessment process; and (3) Provide identified stakeholders with results of the risk assessment, upon completion.	3		RSK-04.4
OIS-08.06B	Application of the Risk Management Policy - Risk Assessment	The analysis, evaluation and treatment of risks, including the approval of actions and acceptance of residual risks, is reviewed by the risk owners for adequacy at least annually. In addition, in case of significant changes to the cloud service, a review is carried out focusing on the parts of the risk assessment relevant to the change.	Functional	Intersects With	Risk Assessment Update	RSK-13.2	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	8		RSK-07
OIS-08.01AS	Application of the Risk Management Policy - Risk Assessment	OIS-08.01AS, sharpening OIS-08.01B The cloud service provider performs the risk management process as specified by OIS-07 as needed and at least annually. The evolution of the risks is monitored and the risk assessments are reviewed correspondingly.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OIS-08.01AS	Application of the Risk Management Policy - Risk Assessment	OIS-08.01AS, sharpening OIS-08.01B The cloud service provider performs the risk management process as specified by OIS-07 as needed and at least annually. The evolution of the risks is monitored and the risk assessments are reviewed correspondingly.	Functional	Intersects With	Risk Monitoring	RSK-22	Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and resilience controls; (2) Changes to the organization's risk profile; and (3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.	5		RSK-11
OIS-08.01AC	Application of the Risk Management Policy - Risk Assessment	The cloud service provider integrates information security risks into a documented Enterprise Risk Management (ERM) programme which addresses the following aspects:	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	8		RSK-01
OIS-08.01AC.1	Application of the Risk Management Policy - Risk Assessment	Integration of information security risks at the enterprise level to promote information security risk-awareness across the entire organisation;	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	3		RSK-01
OIS-08.01AC.2	Application of the Risk Management Policy - Risk Assessment	Leadership awareness and support for identification, analysis and treatment of information security risks to foster continuous improvement; and	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3		GOV-01.2
OIS-08.01AC.3	Application of the Risk Management Policy - Risk Assessment	Consideration of the cloud service provider's strategic objectives when managing risks to align risk treatment with the organisation's goals.	Functional	Intersects With	Risk Framing	RSK-05	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	3		RSK-01.1
OIS-08.02AC	Application of the Risk Management Policy - Risk Assessment	When identifying risks, the cloud service provider also takes into account the detection of unusual and harmful actions of internal threat actors, insofar as it is applicable to the cloud service provided and is within the area of responsibility of the cloud service provider.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
OIS-08.02AC	Application of the Risk Management Policy - Risk Assessment	When identifying risks, the cloud service provider also takes into account the detection of unusual and harmful actions of internal threat actors, insofar as it is applicable to the cloud service provided and is within the area of responsibility of the cloud service provider.	Functional	Intersects With	Insider Threat Program	THR-15	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	5		THR-04
OIS-09.01B	Application of the Risk Management Policy - Risk Treatment	The risk treatment is prioritised corresponding to the level of cybersecurity risks associated with the cloud service.	Functional	Intersects With	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	5		RSK-06
OIS-09.02B	Application of the Risk Management Policy - Risk Treatment	A risk treatment plan according to the risk assessment (cf. OIS-08) is documented and implemented.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-17.1	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	8		RSK-06.4
OIS-09.03B	Application of the Risk Management Policy - Risk Treatment	Actions defined in the risk treatment plan reduce the risk level to a residual risk that risk owners are able to accept.	Functional	Intersects With	Risk Tolerance	RSK-05.1	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	3		RSK-01.3
OIS-09.03B	Application of the Risk Management Policy - Risk Treatment	Actions defined in the risk treatment plan reduce the risk level to a residual risk that risk owners are able to accept.	Functional	Intersects With	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	5		RSK-06
OIS-09.04B	Application of the Risk Management Policy - Risk Treatment	The risk treatment plan, as well as suitably summarised and abstracted versions, is provided to relevant internal parties.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-17.1	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	3		RSK-06.4
OIS-09.05B	Application of the Risk Management Policy - Risk Treatment	Based on contractual agreements and relevant legal and regulatory requirements, the cloud service provider determines which relevant external parties are provided with information, specific to the parties' purposes, about the risk treatment plan. The cloud service provider also determines the extent to which this should happen.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-17.1	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	3		RSK-06.4
OIS-09.06B	Application of the Risk Management Policy - Risk Treatment	The selected options for risk treatment are reviewed by the risk owners every time the risk assessment is modified. The review considers the criteria for risk acceptance and prioritisation of risk treatment.	Functional	Intersects With	Risk Assessment Update	RSK-13.2	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	3		RSK-07
OIS-09.06B	Application of the Risk Management Policy - Risk Treatment	The selected options for risk treatment are reviewed by the risk owners every time the risk assessment is modified. The review considers the criteria for risk acceptance and prioritisation of risk treatment.	Functional	Intersects With	Risk Treatment Options	RSK-16.1	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance and service provider); or (4) Accepting the risk.	5		RSK-06.3
OIS-09.07B	Application of the Risk Management Policy - Risk Treatment	In case of the cloud service provider sharing risks with the cloud service customers, the cloud service provider maps shared risks to complementary customer controls and describes them in the user documentation (cf. PSS-01).	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	5		CLD-06.1
OIS-10.01B	Information Security in Project Management	Information security is integrated into project management. Risks are assessed by the cloud service provider according to OIS-07, and the risk treatment is performed if necessary. Risks are treated in all projects that may have a direct or significant impact on the provision, operation, or security of the cloud service.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	8		PRM-04
5.2	Security Policies and Procedures (SP)	Objective: Provide policies and procedures regarding security requirements and to support business requirements.	Functional	No Relationship	N/A	N/A	N/A	0		
SP-01.01B	Documentation, Communication and Provision of Policies and Procedures	Policies and procedures (incl. frameworks and guidelines) are derived from the information security policy and are documented according to a uniform structure. The policies and procedures describe at least the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8		GOV-02
SP-01.01B.1	Documentation, Communication and Provision of Policies and Procedures	Objectives;	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
SP-01.01B.2	Documentation, Communication and Provision of Policies and Procedures	Scope;	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
SP-01.01B.3	Documentation, Communication and Provision of Policies and Procedures	Roles and responsibilities, including personnel qualification requirements and the establishment of substitution rules;	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03
SP-01.01B.4	Documentation, Communication and Provision of Policies and Procedures	Roles and dependencies on other organisations (especially cloud service customers and subservice organisations);	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-11	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5		TPM-05.4
SP-01.01B.5	Documentation, Communication and Provision of Policies and Procedures	Steps for the execution of the security strategy; and	Functional	Intersects With	Strategic Plan & Objectives	PRM-02	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	3		PRM-01.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
SP-01.01B.6	Documentation, Communication and Provision of Policies and Procedures	Applicable legal and regulatory requirements.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5		CPL-01
SP-01.02B	Documentation, Communication and Provision of Policies and Procedures	The policies and procedures are communicated and made available to all relevant internal and external personnel of the cloud service provider in an appropriate manner.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
SP-01.03B	Documentation, Communication and Provision of Policies and Procedures	The policies and procedures are subject to version control.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
SP-01.04B	Documentation, Communication and Provision of Policies and Procedures	The policies and procedures are approved by the top management of the cloud service provider or an authorised body.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
SP-02.01B	Review and Approval of Policies and Procedures	Information security policies and procedures are reviewed for adequacy by the cloud service provider's subject matter experts at least annually, and in case of significant changes to the cloud service. The review shall consider at least the following aspects:	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and	8		GOV-03
SP-02.01B.1	Review and Approval of Policies and Procedures	Organisational and technical changes in the procedures for providing the cloud service; and	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and	3		GOV-03
SP-02.01B.2	Review and Approval of Policies and Procedures	Legal and regulatory changes in the cloud service provider's environment.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5		CPL-01
SP-02.01B.2	Review and Approval of Policies and Procedures	Legal and regulatory changes in the cloud service provider's environment.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and	3		GOV-03
SP-02.02B	Review and Approval of Policies and Procedures	Revised policies and procedures are approved by the appropriate level of management before they become effective and are communicated and made available to internal and external personnel.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
SP-02.02B	Review and Approval of Policies and Procedures	Revised policies and procedures are approved by the appropriate level of management before they become effective and are communicated and made available to internal and external personnel.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and	3		GOV-03
SP-03.01B	Exceptions from Existing Policies and Procedures	All exceptions to policies and procedures for information security are maintained in a list, including also the controls associated with the exceptions.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and	8		GOV-02.1
SP-03.02B	Exceptions from Existing Policies and Procedures	Exceptions to the policies and procedures for information security as well as respective controls go through risk management procedures in accordance with OIS-07, including approval of these exceptions and acceptance of the associated risks by the risk owners.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5		GOV-02.1
SP-03.02B	Exceptions from Existing Policies and Procedures	Exceptions to the policies and procedures for information security as well as respective controls go through risk management procedures in accordance with OIS-07, including approval of these exceptions and acceptance of the associated risks by the risk owners.	Functional	Intersects With	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	3		RSK-06
SP-03.03B	Exceptions from Existing Policies and Procedures	The risk management procedures in accordance with OIS-07, also take into account the aggregated risk from a combination of single exceptions.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and	3		GOV-02.1
SP-03.03B	Exceptions from Existing Policies and Procedures	The risk management procedures in accordance with OIS-07, also take into account the aggregated risk from a combination of single exceptions.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
SP-03.04B	Exceptions from Existing Policies and Procedures	The approvals of exceptions are documented, with a defined validity and reviewed for appropriateness at least annually by the risk owners or by the top management. This review also takes into account the aggregated risk from a combination of single exceptions.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5		GOV-02.1
SP-03.04B	Exceptions from Existing Policies and Procedures	The approvals of exceptions are documented, with a defined validity and reviewed for appropriateness at least annually by the risk owners or by the top management. This review also takes into account the aggregated risk from a combination of single exceptions.	Functional	Intersects With	Periodic Review of Exceptions	GOV-04.3	Mechanisms exist to: (1) Periodically review previously-approved exceptions; and (2) Determine if the exception should be allowed to	8		
SP-03.05B	Exceptions from Existing Policies and Procedures	Exceptions in information security policies and procedures that would result in a deviation (cf. 3.4.12) from any applicable C5 criterion within the scope of an assurance engagement (cf. 3.4.1) are not permitted.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and	3		GOV-02.1
SP-03.01AC	Exceptions from Existing Policies and Procedures	The exceptions to policies or procedures are approved by the appropriate level of management.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and	5		GOV-02.1
SP-03.02AC	Exceptions from Existing Policies and Procedures	The cloud service provider monitors the list of exceptions to prevent the expiration of approved exceptions and ensure the up-to-dateness of all reviews and approvals.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and	5		GOV-02.1
SP-03.02AC	Exceptions from Existing Policies and Procedures	The cloud service provider monitors the list of exceptions to prevent the expiration of approved exceptions and ensure the up-to-dateness of all reviews and approvals.	Functional	Intersects With	Periodic Review of Exceptions	GOV-04.3	Mechanisms exist to: (1) Periodically review previously-approved exceptions; and (2) Determine if the exception should be allowed to	5		
SP-03.03AC	Exceptions from Existing Policies and Procedures	Any exceptions for which deviations were identified during monitoring are addressed through timely and appropriate remediation measures.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
5.3	Personnel (HR)	Objective: Ensure that personnel understands its responsibilities, is aware of its responsibilities regarding information security, and that the organisation's assets are protected in the event of changes in responsibilities or termination.	Functional	No Relationship	N/A	N/A	N/A	0		
HR-01.01B	Verification of Qualification and Trustworthiness	The cloud service provider identifies for the production environment which roles within the organisation can access cloud service customer data, cloud service derived data, cloud service provider data, account data or system components under the cloud service provider's responsibility.	Functional	Intersects With	Position Categorization	HRS-03	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5		HRS-02
HR-01.01B	Verification of Qualification and Trustworthiness	The cloud service provider identifies for the production environment which roles within the organisation can access cloud service customer data, cloud service derived data, cloud service provider data, account data or system components under the cloud service provider's responsibility.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	3		IAC-08

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
HR-01.02B	Verification of Qualification and Trustworthiness	The competency and integrity of all internal and external personnel to which these roles are assigned is verified prior to employment. The verification considers the following measures, to the extent permitted by local legislation and regulation and as considered appropriate by the cloud service provider to mitigate risks related to inappropriate access to the respective data type:	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	8		HRS-04
HR-01.02B.1	Verification of Qualification and Trustworthiness	Verification of the person's identity via identity card or passport;	Functional	Subset Of	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10		HRS-04
HR-01.02B.2	Verification of Qualification and Trustworthiness	Verification of professional experience through the CV;	Functional	Subset Of	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10		HRS-04
HR-01.02B.3	Verification of Qualification and Trustworthiness	Verification of academic titles and degrees;	Functional	Subset Of	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10		HRS-04
HR-01.02B.4	Verification of Qualification and Trustworthiness	Request for a certificate of good conduct, police clearance or other national equivalents; and	Functional	Subset Of	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10		HRS-04
HR-01.02B.5	Verification of Qualification and Trustworthiness	Evaluation of susceptibility to blackmail.	Functional	Subset Of	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10		HRS-04
HR-01.03B	Verification of Qualification and Trustworthiness	The cloud service provider considers changes in personnel roles or employment status that may impact access rights, responsibilities, or risk exposure, and identifies and mitigates related risks.	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-08	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	5		HRS-01.1
HR-01.03B	Verification of Qualification and Trustworthiness	The cloud service provider considers changes in personnel roles or employment status that may impact access rights, responsibilities, or risk exposure, and identifies and mitigates related risks.	Functional	Intersects With	Personnel Transfer	HRS-11	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	5		HRS-08
HR-01.04B	Verification of Qualification and Trustworthiness	The cloud service provider classifies security-sensitive positions according to their level of risk, including IT administration roles and any positions with access to cloud service customer data or to system components used to provide the cloud service in the production environment.	Functional	Intersects With	Position Categorization	HRS-03	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	8		HRS-02
HR-01.04B	Verification of Qualification and Trustworthiness	The cloud service provider classifies security-sensitive positions according to their level of risk, including IT administration roles and any positions with access to cloud service customer data or to system components used to provide the cloud service in the production environment.	Functional	Intersects With	Users With Elevated Privileges	HRS-03.1	Mechanisms exist to ensure that every user accessing Technology Assets, Applications and/or Services (TAAS) that process, store and/or transmit sensitive and/or regulated data is cleared and regularly trained to handle the information in	5		HRS-02.1
HR-01.05B	Verification of Qualification and Trustworthiness	The cloud service provider assesses the competence and integrity of its personnel before transfer or promotion into a role with a higher risk classification.	Functional	Intersects With	Roles With Special Protection Measures	HRS-05.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5		HRS-04.1
HR-01.05B	Verification of Qualification and Trustworthiness	The cloud service provider assesses the competence and integrity of its personnel before transfer or promotion into a role with a higher risk classification.	Functional	Intersects With	Personnel Transfer	HRS-11	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	3		HRS-08
HR-01.06B	Verification of Qualification and Trustworthiness	The intensity of the assessment defined in this criterion is in proportion to the business context, the sensitivity of the information that the personnel will access, and the associated risks.	Functional	Intersects With	Position Categorization	HRS-03	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	3		HRS-02
HR-01.06B	Verification of Qualification and Trustworthiness	The intensity of the assessment defined in this criterion is in proportion to the business context, the sensitivity of the information that the personnel will access, and the associated risks.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04
HR-01.01AC	Verification of Qualification and Trustworthiness	The cloud service provider defines in the human resource policy positions with levels and risk classification that require regular assessment of competence and integrity. The cloud service provider annually reviews their assessment of competence and integrity for personnel belonging to the defined positions.	Functional	Intersects With	Roles With Special Protection Measures	HRS-05.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5		HRS-04.1
HR-02.01B	Employment Terms and Conditions	The cloud service provider ensures that the employment terms and conditions reflect applicable legal and regulatory requirements in accordance with SP-01.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
HR-02.01B	Employment Terms and Conditions	The cloud service provider ensures that the employment terms and conditions reflect applicable legal and regulatory requirements in accordance with SP-01.	Functional	Intersects With	Terms of Employment	HRS-06	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5		HRS-05
HR-02.02B	Employment Terms and Conditions	The cloud service provider's internal and external personnel are required by employment terms and conditions to comply with the code of ethics and the information security policy, as well as the policies, procedures and instructions based on it.	Functional	Intersects With	Terms of Employment	HRS-06	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5		HRS-05
HR-02.02B	Employment Terms and Conditions	The cloud service provider's internal and external personnel are required by employment terms and conditions to comply with the code of ethics and the information security policy, as well as the policies, procedures and instructions based on it.	Functional	Intersects With	Rules of Behavior	HRS-06.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5		HRS-05.1
HR-02.03B	Employment Terms and Conditions	The cloud service provider ensures that a non-disclosure provision is included in the terms for all internal and external personnel. The non-disclosure provision covers any information, including anonymised and decontextualised information, that the personnel obtains or generates as part of the cloud service.	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	8		HRS-06.1
HR-02.04B	Employment Terms and Conditions	The cloud service provider instructs its personnel on the code of ethics and the information security policy, as well as the policies, procedures and instructions based on it, before access is granted to any cloud service customer data, cloud service derived data, cloud service provider data and account data or system components under the responsibility of the cloud service provider used to provide the cloud service in the production environment.	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-08.2	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	5		HRS-05.7
HR-02.04B	Employment Terms and Conditions	The cloud service provider instructs its personnel on the code of ethics and the information security policy, as well as the policies, procedures and instructions based on it, before access is granted to any cloud service customer data, cloud service derived data, cloud service provider data and account data or system components under the responsibility of the cloud service provider used to provide the cloud service in the production environment.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3		SAT-02
HR-02.05B	Employment Terms and Conditions	Additionally, the cloud service provider requires the code of ethics and the information security policy, as well as the policies, procedures and instructions based on it, to be acknowledged by the internal and external personnel in a documented form before access is granted to any of the aforementioned data or system components.	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-08.2	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	8		HRS-05.7
HR-03.01B	Security Training and Awareness Programme	The cloud service provider operates a target group-oriented security awareness and training programme.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-02	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5		SAT-01
HR-03.01B	Security Training and Awareness Programme	The cloud service provider operates a target group-oriented security awareness and training programme.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		SAT-02
HR-03.02B	Security Training and Awareness Programme	All internal and external personnel of the cloud service provider undergoes a role-based training programme regularly and when changing job function, taking into consideration at least the risk classification and technical responsibilities of their position.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8		SAT-03

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
HR-03.03B	Security Training and Awareness Programme	The programme is regularly updated based on changes to policies and procedures and the current threat situation and includes the following aspects insofar as they are applicable to each personnel's role:	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-03	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	5		SAT-01.1
HR-03.03B.1	Security Training and Awareness Programme	Handling system components used to provide the cloud service in the production environment in accordance with applicable policies and procedures;	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03
HR-03.03B.2	Security Training and Awareness Programme	Handling cloud service customer data, cloud service derived data, cloud service provider data and account data in accordance with applicable policies and procedures and applicable legal and regulatory requirements;	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-05.1	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive and/or regulated data is formally trained in data handling requirements.	5		SAT-03.3
HR-03.03B.3	Security Training and Awareness Programme	Information about the current threat situation;	Functional	Intersects With	Cyber Threat Environment Situational Awareness	SAT-06	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5		SAT-03.6
HR-03.03B.4	Security Training and Awareness	Correct behaviour in the event of security incidents;	Functional	Intersects With	Incident Response Training	IRO-10	Mechanisms exist to train personnel in their incident response roles and responsibilities.	3		IRO-05
HR-03.03B.4	Security Training and Awareness Programme	Correct behaviour in the event of security incidents;	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-06.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5		SAT-03.2
HR-03.03B.5	Security Training and Awareness Programme	Security best practices; and	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3		SAT-02
HR-03.03B.6	Security Training and Awareness Programme	Secure development.	Functional	Intersects With	Continuing Professional Education (CPE) - DevOps Personnel	SAT-08	Mechanisms exist to ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure Software Development Practices (SSDP) to appropriately address evolving threats.	5		SAT-03.8
HR-03.04B	Security Training and Awareness Programme	The learning outcomes achieved through the awareness and training programme are measured and evaluated.	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-10	Mechanisms exist to document, retain and monitor individual training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets, Applications and/or Services (TAAS)-specific training.	5		SAT-04
HR-03.02AS	Security Training and Awareness Programme	HR-03.02AS, sharpening HR-03.02B All internal and external personnel of the cloud service provider undergoes a role-based training programme at least annually and when changing job function, taking into consideration at least the risk classification and technical responsibilities of their position.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8		SAT-03
HR-03.01AC	Security Training and Awareness Programme	The cloud service provider monitors the completion of the security awareness and training programme.	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-10	Mechanisms exist to document, retain and monitor individual training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets, Applications and/or Services (TAAS)-specific training.	5		SAT-04
HR-03.02AC	Security Training and Awareness Programme	Timely and appropriate remediation measures address any deviations identified during monitoring.	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-10	Mechanisms exist to document, retain and monitor individual training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets, Applications and/or Services (TAAS)-specific training.	3		SAT-04
HR-03.03AC	Security Training and Awareness Programme	The learning outcomes achieved through the awareness and training programme are measured and evaluated in a target group-oriented manner.	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-10	Mechanisms exist to document, retain and monitor individual training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets, Applications and/or Services (TAAS)-specific training.	3		SAT-04
HR-03.04AC	Security Training and Awareness Programme	The measurements cover quantitative and qualitative aspects.	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-10	Mechanisms exist to document, retain and monitor individual training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets, Applications and/or Services (TAAS)-specific training.	3		SAT-04
HR-03.05AC	Security Training and Awareness Programme	The results are used to improve the awareness and training programme.	Functional	Intersects With	Training Feedback	SAT-11	Mechanisms exist to: (1) Monitor individual training results; and (2) Report findings to stakeholders.	5		SAT-04.1
HR-04.01B	Disciplinary Measures	The cloud service provider ensures that the policies and procedures concerning disciplinary measures reflect applicable legal and regulatory requirements in accordance with SP-01.	Functional	Intersects With	Personnel Sanctions	HRS-10	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5		HRS-07
HR-04.02B	Disciplinary Measures	In the event of violations of policies and procedures or applicable legal and regulatory requirements, actions are taken in accordance with a defined policy that includes the following aspects:	Functional	Intersects With	Personnel Sanctions	HRS-10	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5		HRS-07
HR-04.02B.1	Disciplinary Measures	Verifying whether a violation has occurred; and	Functional	Intersects With	Workplace Investigations	HRS-10.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	5		HRS-07.1
HR-04.02B.2	Disciplinary Measures	Consideration of the nature and severity of the violation and its impact.	Functional	Intersects With	Personnel Sanctions	HRS-10	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	3		HRS-07
HR-04.03B	Disciplinary Measures	The internal and external personnel of the cloud service provider is informed about possible disciplinary measures.	Functional	Intersects With	Personnel Sanctions	HRS-10	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5		HRS-07
HR-04.04B	Disciplinary Measures	The use of disciplinary measures is appropriately documented.	Functional	Intersects With	Personnel Sanctions	HRS-10	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5		HRS-07
HR-05.01B	Responsibilities in the Event of Termination or Change of Employment	Internal and external personnel has been informed about which responsibilities, arising from employment terms and conditions relating to information security, will remain in place when the employment is terminated or changed and for how long.	Functional	Intersects With	Post-Employment Requirements Awareness	HRS-08.3	Mechanisms exist to notify individuals of their applicable, legally-binding post-employment requirements for the protection of sensitive and/or regulated data.	5		HRS-06.2
HR-05.01B	Responsibilities in the Event of Termination or Change of Employment	Internal and external personnel has been informed about which responsibilities, arising from employment terms and conditions relating to information security, will remain in place when the employment is terminated or changed and for how long.	Functional	Intersects With	Post-Employment Requirements Notification	HRS-08.4	Mechanisms exist to govern former employee behavior by formally notifying terminated individuals of their applicable, legally binding post-employment requirements for the protection of sensitive and/or regulated data.	5		HRS-09.3
HR-06.01B	Non-disclosure Agreements	The non-disclosure or confidentiality agreements to be agreed with internal personnel and service organisations of the cloud service provider are based on the requirements identified by the cloud service provider for the protection of confidential information and operational details.	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	8		HRS-06.1
HR-06.02B	Non-disclosure Agreements	The agreements are to be accepted by service organisations when the contract is agreed.	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	5		HRS-06.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
HR-06.02B	Non-disclosure Agreements	The agreements are to be accepted by service organisations when the contract is agreed.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
HR-06.03B	Non-disclosure Agreements	The agreements are to be accepted by internal personnel of the cloud service provider before authorisation to access cloud service customer data, cloud service derived data, cloud service provider data and account data is granted.	Functional	Intersects With	Access Agreements	HRS-07	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	3		HRS-06
HR-06.03B	Non-disclosure Agreements	The agreements are to be accepted by internal personnel of the cloud service provider before authorisation to access cloud service customer data, cloud service derived data, cloud service provider data and account data is granted.	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	5		HRS-06.1
HR-06.04B	Non-disclosure Agreements	The requirements are documented and reviewed at regular intervals (at least annually), as well as in case of significant changes to the cloud service. If the review shows that the requirements need to be adapted, the non-disclosure or confidentiality agreements are updated.	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	5		HRS-06.1
HR-06.05B	Non-disclosure Agreements	The cloud service provider informs the internal personnel and service organisations and obtains confirmation of the updated confidentiality or non-disclosure agreement.	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	3		HRS-06.1
HR-06.06B	Non-disclosure Agreements	In instances where an agreement on the updates cannot be reached, the cloud service provider assesses the resulting risks to information security according to OIS-07.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
HR-07.01B	Remote Working - Policy	Policies and procedures for the protection of information when personnel works remotely are documented, communicated and provided in accordance with SP-01 and address the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8		GOV-02
HR-07.01B	Remote Working - Policy	Policies and procedures for the protection of information when personnel works remotely are documented, communicated and provided in accordance with SP-01 and address the following aspects:	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-27	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5		NET-14.5
HR-07.01B.1	Remote Working - Policy	Establishing guidelines for the personnel for the safe handling and storage of sensitive information and data types;	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	3		DCH-01
HR-07.01B.1	Remote Working - Policy	Establishing guidelines for the personnel for the safe handling and storage of sensitive information and data types;	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-05.1	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive and/or regulated data is formally trained in data handling requirements.	3		SAT-03.3
HR-07.01B.2	Remote Working - Policy	Definition of remote access security requirements;	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		NET-14
HR-07.01B.3	Remote Working - Policy	Utilisation of secure communication methods and enforcement of secure network use (e.g., VPN usage, endpoint protection, multi-factor authentication, secure communication channels); and	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	3		IAC-06
HR-07.01B.3	Remote Working - Policy	Utilisation of secure communication methods and enforcement of secure network use (e.g., VPN usage, endpoint protection, multi-factor authentication, secure communication channels); and	Functional	Intersects With	Remote Access Cryptographic Protections	NET-26.5	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	5		NET-14.2
HR-07.01B.4	Remote Working - Policy	Provision of organisation-approved equipment and prohibition of unregulated personal devices.	Functional	Intersects With	Usage Parameters	AST-28	Mechanisms exist to monitor and enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of system settings.	3		AST-14
HR-07.01B.4	Remote Working - Policy	Provision of organisation-approved equipment and prohibition of unregulated personal devices.	Functional	Intersects With	Technology Use Restrictions	HRS-06.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5		HRS-05.3
HR-08.01B	Remote Working - Implementation	The cloud service provider designs, implements and maintains the technical and organisational measures required to enable its personnel to comply with the policies and procedures for remote work (cf. HR-07).	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3		NET-14
HR-08.01B	Remote Working - Implementation	The cloud service provider designs, implements and maintains the technical and organisational measures required to enable its personnel to comply with the policies and procedures for remote work (cf. HR-07).	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-27	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5		NET-14.5
5.4	Asset Management (AM)	Objective: Identify the organisation's own assets and ensure an appropriate level of protection throughout their lifecycle.	Functional	No Relationship	N/A	N/A	N/A	0		
AM-01.01B	Asset Management Framework	An asset management framework is documented, communicated and provided according to SP-01, in which the following aspects are described:	Functional	Intersects With	Asset Management Policy	AST-01	Mechanisms exist to establish a formal, documented asset management policy that: (1) Conveys executive management's intent;	8		
AM-01.01B	Asset Management Framework	An asset management framework is documented, communicated and provided according to SP-01, in which the following aspects are described:	Functional	Intersects With	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	8		AST-01
AM-01.01B.1	Asset Management Framework	Identification of assets which are used to provide the cloud service in the production environment;	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02
AM-01.01B.2	Asset Management Framework	Definition of a scheme for identifying protection needs based on information processed, stored or transmitted on the asset;	Functional	Intersects With	Asset Categorization	AST-15	Mechanisms exist to categorize Technology Assets, Applications and/or Services (TAAS).	3		AST-31
AM-01.01B.2	Asset Management Framework	Definition of a scheme for identifying protection needs based on information processed, stored or transmitted on the asset;	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02
AM-01.01B.3	Asset Management Framework	Definition of asset types, considering at a minimum the differentiation of hardware and software objects;	Functional	Intersects With	Asset Categorization	AST-15	Mechanisms exist to categorize Technology Assets, Applications and/or Services (TAAS).	5		AST-31
AM-01.01B.4	Asset Management Framework	Definition of asset lifecycles based on the asset type; and	Functional	Intersects With	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	3		AST-01

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
AM-01.01B.5	Asset Management Framework	Definition of procedures for inventory of hardware and software assets.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02
AM-01.01AC	Asset Management Framework	The information collected about assets is considered in logging and monitoring applications to:	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	3		AST-02
AM-01.01AC	Asset Management Framework	The information collected about assets is considered in logging and monitoring applications to:	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
AM-01.01AC.1	Asset Management Framework	Identify the impact on cloud services and functions in case of events that could lead to a breach of protection objectives; and	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
AM-01.01AC.1	Asset Management Framework	Identify the impact on cloud services and functions in case of events that could lead to a breach of protection objectives; and	Functional	Intersects With	Impact-Level Prioritization	RSK-07.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	3		RSK-02.1
AM-01.01AC.2	Asset Management Framework	Support information provided to affected cloud service customers in accordance with contractual agreements.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	3		IRO-10
AM-01.02AC	Asset Management Framework	The cloud service provider assures that the inventory of assets is up-to-date by implementing monitoring measures to the process that is maintaining it.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02
AM-01.02AC	Asset Management Framework	The cloud service provider assures that the inventory of assets is up-to-date by implementing monitoring measures to the process that is maintaining it.	Functional	Intersects With	Comprehensive Asset Inventory Management	AST-08	Mechanisms exist to maintain a dynamically updated inventory of Technology Assets, Applications, Services and/or Data (TAASD) that provides a highly contextualized understanding of every asset that is capable of providing operational visibility required to: (1) Detect anomalies; (2) Manage complex vulnerabilities;	5		
AM-02.01B	Asset Inventory	The cloud service provider maintains an asset inventory of hardware and software assets in accordance with the asset management framework (cf. AM-01).	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8		AST-02
AM-02.02B	Asset Inventory	The inventory is performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02
AM-02.02B	Asset Inventory	The inventory is performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Functional	Intersects With	Comprehensive Asset Inventory Management	AST-08	Mechanisms exist to maintain a dynamically updated inventory of Technology Assets, Applications, Services and/or Data (TAASD) that provides a highly contextualized understanding of every asset that is capable of providing operational visibility required to: (1) Detect anomalies;	5		
AM-02.02B	Asset Inventory	The inventory is performed automatically and/or by the people or teams responsible for the assets to ensure complete, accurate, valid and consistent inventory throughout the asset lifecycle.	Functional	Intersects With	Automated Network Asset Discovery	AST-09.2	Mechanisms exist to automate network asset discovery through Software Defined Networking (SDN), or similar technologies, that analyzes network traffic to: (1) Identify; (2) Document; and (3) Track devices.	3		AST-32
AM-02.03B	Asset Inventory	Assets are recorded with the information needed to apply the risk management procedure (cf. OIS-07), including the measures taken to manage these risks throughout the asset lifecycle.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
AM-02.03B	Asset Inventory	Assets are recorded with the information needed to apply the risk management procedure (cf. OIS-07), including the measures taken to manage these risks throughout the asset lifecycle.	Functional	Intersects With	Risk-Based Security Categorization	RSK-07	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	3		RSK-02
AM-02.04B	Asset Inventory	Changes to the recorded information of an asset are logged.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	3		AST-02
AM-02.04B	Asset Inventory	Changes to the recorded information of an asset are logged.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
AM-02.05B	Asset Inventory	The cloud service provider maintains lists of all users under its responsibility who have access to a specific resource, along with their respective access rights.	Functional	Intersects With	User & Service Account Inventories	IAC-08.3	Mechanisms exist to maintain a current list of authorized users and service accounts.	5		IAC-01.3
AM-02.05B	Asset Inventory	The cloud service provider maintains lists of all users under its responsibility who have access to a specific resource, along with their respective access rights.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	3		IAC-17
AM-03.01B	Hardware Asset Inventory	The hardware asset inventory maintained by the cloud service provider (cf. AM-02) includes information for each entry that:	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8		AST-02
AM-03.01B.1	Hardware Asset Inventory	Enables the identification of the hardware asset;	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02
AM-03.01B.2	Hardware Asset Inventory	Provides visibility into the lifecycle of the hardware asset; and	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	3		AST-02
AM-03.01B.3	Hardware Asset Inventory	Enables the cloud service provider to control the hardware asset, perform a risk assessment and protect its information security.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	3		AST-02
AM-03.01B.3	Hardware Asset Inventory	Enables the cloud service provider to control the hardware asset, perform a risk assessment and protect its information security.	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment	AST-07.1	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	3		AST-03
AM-04.01B	Software Asset Inventory	The cloud service provider maintains a comprehensive inventory of all software assets, including used software (cf. AM-02). This inventory includes information for each entry that:	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8		AST-02
AM-04.01B	Software Asset Inventory	The cloud service provider maintains a comprehensive inventory of all software assets, including used software (cf. AM-02). This inventory includes information for each entry that:	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	3		TDA-04.2

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
AM-04.01B.1	Software Asset Inventory	Enables the identification of the software asset;	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02
AM-04.01B.2	Software Asset Inventory	Provides visibility into which other assets use the software asset for the provision of the cloud service; and	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5		TDA-04.2
AM-04.01B.3	Software Asset Inventory	Enables the cloud service provider to control the software asset, perform a risk assessment and protect its information security.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	3		AST-02
AM-04.01B.3	Software Asset Inventory	Enables the cloud service provider to control the software asset, perform a risk assessment and protect its information security.	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment	AST-07.1	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	3		AST-03
AM-04.01AC	Software Asset Inventory	The inventory also includes information for each entry that provides visibility into how long the software asset will receive security updates from its supplier, if such a time frame has been communicated by the supplier.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required	5		TDA-17
AM-05.01B	Policy for the Proper and Secure Use of Assets	Policies and procedures for the proper and secure use of assets are documented, communicated and provided in accordance with SP-01 and address the following aspects of the asset lifecycle as applicable to the asset:	Functional	Intersects With	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5		AST-01
AM-05.01B	Policy for the Proper and Secure Use of Assets	Policies and procedures for the proper and secure use of assets are documented, communicated and provided in accordance with SP-01 and address the following aspects of the asset lifecycle as applicable to the asset:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8		GOV-02
AM-05.01B.1	Policy for the Proper and Secure Use of Assets	Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorised personnel or system components;	Functional	Intersects With	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	3		AST-01
AM-05.01B.1	Policy for the Proper and Secure Use of Assets	Approval procedures for acquisition, commissioning, maintenance, decommissioning, and disposal by authorised personnel or system components;	Functional	Intersects With	Decommissioning	AST-36	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that: (1) Data is properly transitioned to new systems or archived; and (2) Hard drives are either destroyed or erased in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	3		AST-30
AM-05.01B.2	Policy for the Proper and Secure Use of Assets	Classification and labelling based on the protection need of the cloud service customer data, cloud service derived data, cloud service provider data and account data as well as measures for the level of protection identified;	Functional	Intersects With	Asset Scope Classification	AST-16	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	3		AST-04.1
AM-05.01B.2	Policy for the Proper and Secure Use of Assets	Classification and labelling based on the protection need of the cloud service customer data, cloud service derived data, cloud service provider data and account data as well as measures for the level of protection identified;	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02
AM-05.01B.3	Policy for the Proper and Secure Use of Assets	Secure configuration of mechanisms for error handling, logging, encryption, authentication and authorisation;	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02
AM-05.01B.4	Policy for the Proper and Secure Use of Assets	Requirements for versions of software and images as well as application of patches;	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
AM-05.01B.5	Policy for the Proper and Secure Use of Assets	Handling of software for which support and security patches are not available anymore;	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required	5		TDA-17
AM-05.01B.6	Policy for the Proper and Secure Use of Assets	Restriction of software installations or use of services;	Functional	Intersects With	Restrict Roles Permitted To Install Software	CFG-12	Automated mechanisms exist to prevent the installation of software, unless the action is performed by a privileged user or service.	5		CFG-05
AM-05.01B.6	Policy for the Proper and Secure Use of Assets	Restriction of software installations or use of services;	Functional	Intersects With	Role-Based Permissions To Implement Changes	CHG-04.2	Mechanisms exist to limit the ability to implement Technology Asset, Application and/or Service (TAAS) changes to designated privileged roles.	3		END-03
AM-05.01B.7	Policy for the Proper and Secure Use of Assets	Protection against malware;	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04
AM-05.01B.8	Policy for the Proper and Secure Use of Assets	Remote deactivation, deletion or blocking;	Functional	Intersects With	Remote Purging	MDM-09	Mechanisms exist to remotely purge selected information from mobile devices.	5		MDM-05
AM-05.01B.9	Policy for the Proper and Secure Use of Assets	Physical delivery and transport;	Functional	Intersects With	Removal of Assets	AST-24	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	5		AST-11
AM-05.01B.9	Policy for the Proper and Secure Use of Assets	Physical delivery and transport;	Functional	Intersects With	Media Transportation	DCH-16	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security	3		DCH-07
AM-05.01B.10	Policy for the Proper and Secure Use of Assets	Dealing with incidents and vulnerabilities;	Functional	Intersects With	Incident Response Operations	IRO-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	3		IRO-01
AM-05.01B.10	Policy for the Proper and Secure Use of Assets	Dealing with incidents and vulnerabilities;	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	3		VPM-01

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
AM-05.01B.11	Policy for the Proper and Secure Use of Assets	Deletion of cloud service customer data, cloud service derived data, cloud service provider data and account data; and	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	3		DCH-21
AM-05.01B.11	Policy for the Proper and Secure Use of Assets	Deletion of cloud service customer data, cloud service derived data, cloud service provider data and account data; and	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5		DCH-09
AM-05.01B.12	Policy for the Proper and Secure Use of Assets	Secure handling and usage of removable media, e.g. by specifying which devices are permitted to interact with removable media and what data can be stored on them or by banning the reuse of removable media.	Functional	Intersects With	Digital Media Use Restrictions	DCH-19	Mechanisms exist to restrict the use of types of digital media on systems or system components.	3		DCH-10
AM-05.01B.12	Policy for the Proper and Secure Use of Assets	Secure handling and usage of removable media, e.g. by specifying which devices are permitted to interact with removable media and what data can be stored on them or by banning the reuse of removable media.	Functional	Intersects With	Removable Media Security	DCH-21	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5		DCH-12
AM-05.02B	Policy for the Proper and Secure Use of Assets	The applicability of these aspects is defined based on the cloud service provider's asset management framework (cf. AM-01).	Functional	Intersects With	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	3		AST-01
AM-06.01B	Commissioning of Hardware	The cloud service provider has implemented an approval process for commissioning hardware used to provide the cloud service in the production environment. This process involves identifying, analysing, and mitigating any risks (cf. OIS-07) associated with the	Functional	Intersects With	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	3		AST-01
AM-06.01B	Commissioning of Hardware	The cloud service provider has implemented an approval process for commissioning hardware used to provide the cloud service in the production environment. This process involves identifying, analysing, and mitigating any risks (cf. OIS-07) associated with the commissioning.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
AM-06.02B	Commissioning of Hardware	Approval is granted after verification of the secure configuration of the mechanisms for error handling, logging, encryption, authentication and authorisation according to the intended use and based on the applicable policies.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02
AM-07.01B	Decommissioning of Hardware	The cloud service provider defines, documents and implements a procedure for the decommissioning of hardware used to operate system components supporting the cloud service production environment under the responsibility of the cloud service provider. As part of this procedure, approval by authorised personnel of the cloud service provider based on the applicable policies is required.	Functional	Intersects With	Decommissioning	AST-36	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that: (1) Data is properly transitioned to new systems or archived; and (2) Hard drives are either destroyed or erased in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	8		AST-30
AM-07.02B	Decommissioning of Hardware	The decommissioning includes either:	Functional	Intersects With	Decommissioning	AST-36	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that: (1) Data is properly transitioned to new systems or archived; and (2) Hard drives are either destroyed or erased in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5		AST-30
AM-07.02B.1	Decommissioning of Hardware	The complete and permanent deletion of all cloud service customer data, cloud service derived data, cloud service provider data and account data; or	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5		DCH-09
AM-07.02B.2	Decommissioning of Hardware	The proper destruction of the media.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	3		AST-09
AM-07.02B.2	Decommissioning of Hardware	The proper destruction of the media.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08
AM-07.02B.3	Decommissioning of Hardware	Account data needs to be deleted at least in cases where the data is located in the production environment for the operation of system components.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	3		DCH-09
AM-07.01AS	Decommissioning of Hardware	AM-07.01AS, sharpening AM-07.01B The cloud service provider defines, documents and implements a procedure for the decommissioning of hardware used to operate system components supporting the cloud service production, development, test or staging environment under the responsibility of the cloud service provider. As part of this procedure, approval by authorised personnel of the cloud service provider based on the applicable policies is required.	Functional	Intersects With	Decommissioning	AST-36	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that: (1) Data is properly transitioned to new systems or archived; and (2) Hard drives are either destroyed or erased in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	8		AST-30
AM-07.01AC	Decommissioning of Hardware	The destruction of data on hardware components is carried out in such a manner that data recovery can be reasonably considered to be impossible.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	5		AST-09
AM-07.01AC	Decommissioning of Hardware	The destruction of data on hardware components is carried out in such a manner that data recovery can be reasonably considered to be impossible.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	8		DCH-09
AM-08.01B	Commitment to Proper Use, Safe and Secure Handling and Return of Assets	The cloud service provider determines in a risk assessment (cf. OIS-07) if loss of or unauthorised access to assets could compromise the information security of the cloud service. If so, the cloud service provider's internal and external personnel is provably committed to the policies and procedures for proper use and safe and secure handling of assets before they can be used.	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-08.2	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	5		HRS-05.7
AM-08.01B	Commitment to Proper Use, Safe and Secure Handling and Return of Assets	The cloud service provider determines in a risk assessment (cf. OIS-07) if loss of or unauthorised access to assets could compromise the information security of the cloud service. If so, the cloud service provider's internal and external personnel is provably committed to the policies and procedures for proper use and safe and secure handling of assets before they can be used.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
AM-08.02B	Commitment to Proper Use, Safe and Secure Handling and Return of Assets	Any assets handed over are provably returned upon termination of employment.	Functional	Intersects With	Return of Assets	AST-23	Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.	5		AST-10
AM-08.02B	Commitment to Proper Use, Safe and Secure Handling and Return of Assets	Any assets handed over are provably returned upon termination of employment.	Functional	Intersects With	Asset Collection	HRS-12.2	Mechanisms exist to retrieve organization-owned assets upon termination of an individual's employment.	8		HRS-09.1
AM-08.03B	Commitment to Proper Use, Safe and Secure Handling and Return of Assets	If assets cannot be returned prior to or on the day of the termination, the cloud service provider removes the access rights of the personnel no later than the date of termination	Functional	Intersects With	Personnel Termination	HRS-12	Mechanisms exist to govern the termination of individual employment.	5		HRS-09

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
AM-08.03B	Commitment to Proper Use, Safe and Secure Handling and Return of Assets	If assets cannot be returned prior to or on the day of the termination, the cloud service provider removes the access rights of the personnel no later than the date of termination	Functional	Intersects With	Termination of Employment	IAC-04.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	3		IAC-07.2
AM-09.01B	Asset Classification and Labelling	Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the category of cloud service customer data, cloud service derived data, cloud service provider data and account data it processes, stores, or transmits.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	8		DCH-02
AM-09.01B	Asset Classification and Labelling	Assets are classified and, if possible, labelled. Classification and labelling of an asset reflect the protection needs of the category of cloud service customer data, cloud service derived data, cloud service provider data and account data it processes, stores, or transmits.	Functional	Intersects With	Media Marking	DCH-11	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5		DCH-04
AM-09.02B	Asset Classification and Labelling	Classification levels are reviewed at least annually and in case of significant changes to the cloud service. Based on the review, the classification levels are updated where appropriate.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02
AM-09.03B	Asset Classification and Labelling	The protection need is determined by the individuals or groups responsible for the assets of the cloud service provider according to a uniform and documented classification schema.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	3		DCH-02
AM-09.03B	Asset Classification and Labelling	The protection need is determined by the individuals or groups responsible for the assets of the cloud service provider according to a uniform and documented classification schema.	Functional	Intersects With	Data Stewardship	DCH-06	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5		DCH-01.1
AM-09.04B	Asset Classification and Labelling	The classification schema provides levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. These protection objectives are aligned with delivery and recovery objectives set out in business and disaster recovery plans.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	3		DCH-02
AM-09.04B	Asset Classification and Labelling	The classification schema provides levels of protection for the confidentiality, integrity, availability, and authenticity protection objectives. These protection objectives are aligned with delivery and recovery objectives set out in business and disaster recovery plans.	Functional	Intersects With	Risk-Based Security Categorization	RSK-07	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	3		RSK-02
AM-09.01AC	Asset Classification and Labelling	The unique identification of physical devices serves as an additional method for connection authentication.	Functional	Intersects With	Identification & Authentication for Devices	IAC-34	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5		IAC-04
AM-09.02AC	Asset Classification and Labelling	Device identification is integrated into the asset classification and labeling processes.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	3		DCH-02
AM-09.02AC	Asset Classification and Labelling	Device identification is integrated into the asset classification and labeling processes.	Functional	Intersects With	Identification & Authentication for Devices	IAC-34	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	3		IAC-04
AM-09.03AC	Asset Classification and Labelling	Logging and monitoring applications take the asset protection needs into account in order to inform the responsible stakeholder of events that could lead to a violation of the protection goals, so that the necessary measures are taken with an appropriate priority.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
AM-09.03AC	Asset Classification and Labelling	Logging and monitoring applications take the asset protection needs into account in order to inform the responsible stakeholder of events that could lead to a violation of the protection goals, so that the necessary measures are taken with an appropriate priority.	Functional	Intersects With	Impact-Level Prioritization	RSK-07.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	3		RSK-02.1
AM-09.04AC	Asset Classification and Labelling	Actions for events on assets with a higher level of protection take precedence over events on assets with a lower protection need.	Functional	Intersects With	Impact-Level Prioritization	RSK-07.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5		RSK-02.1
AM-10.01B	Protection of Hardware on Hold	Based on a risk assessment (cf. OIS-07), the cloud service provider has documented and implemented a procedure for protecting hardware components of the cloud service's production environment that are temporarily not in use. The procedure supports the secure storage and protection against unauthorised access or damage of inactive hardware until it is needed again.	Functional	Intersects With	Security of Assets & Media	AST-18	Mechanisms exist to maintain strict control over Technology Assets, Applications, Services and/or Data (TAASD) to preserve confidentiality and integrity.	5		AST-05
AM-10.01B	Protection of Hardware on Hold	Based on a risk assessment (cf. OIS-07), the cloud service provider has documented and implemented a procedure for protecting hardware components of the cloud service's production environment that are temporarily not in use. The procedure supports the secure storage and protection against unauthorised access or damage of inactive hardware until it is needed again.	Functional	Intersects With	Media Storage	DCH-13	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	3		DCH-06
AM-10.01AS	Protection of Hardware on Hold	AM-10.01AS, sharpening AM-10.01B Based on a risk assessment (cf. OIS-07), the cloud service provider has documented and implemented a procedure for protecting any hardware components that are temporarily not in use. The procedure supports the secure storage and protection against unauthorised access or damage of inactive hardware until it is needed again.	Functional	Intersects With	Security of Assets & Media	AST-18	Mechanisms exist to maintain strict control over Technology Assets, Applications, Services and/or Data (TAASD) to preserve confidentiality and integrity.	5		AST-05
AM-10.01AS	Protection of Hardware on Hold	AM-10.01AS, sharpening AM-10.01B Based on a risk assessment (cf. OIS-07), the cloud service provider has documented and implemented a procedure for protecting any hardware components that are temporarily not in use. The procedure supports the secure storage and protection against unauthorised access or damage of inactive hardware until it is needed again.	Functional	Intersects With	Media Storage	DCH-13	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	3		DCH-06
AM-11.01B	Transfer of Hardware	Based on a risk assessment (cf. OIS-07), the cloud service provider ensures the secure and controlled transfer of hardware objects used in the cloud service production environment to an offsite or alternate location.	Functional	Intersects With	Removal of Assets	AST-24	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	8		AST-11
AM-11.02B	Transfer of Hardware	The transfer of hardware is authorised by designated personnel.	Functional	Intersects With	Removal of Assets	AST-24	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	5		AST-11
AM-11.03B	Transfer of Hardware	The cloud service provider ensures that all transfers of hardware objects used in the cloud service production environment are conducted using secure, documented methods designed to prevent unauthorised access, tampering, data leakage, or loss during transit. These methods include physical protection, chain-of-custody tracking, and verification upon receipt.	Functional	Intersects With	Removal of Assets	AST-24	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	5		AST-11
AM-11.03B	Transfer of Hardware	The cloud service provider ensures that all transfers of hardware objects used in the cloud service production environment are conducted using secure, documented methods designed to prevent unauthorised access, tampering, data leakage, or loss during transit. These methods include physical protection, chain-of-custody tracking, and verification upon receipt.	Functional	Intersects With	Media Transportation	DCH-16	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5		DCH-07
AM-12.01B	Removable Media and Endpoint Devices	Based on a risk assessment (cf. OIS-07), the cloud service provider designs, implements and maintains controls for endpoint devices and removable storage media regarding the following aspects:	Functional	Intersects With	Removable Media Security	DCH-21	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5		DCH-12
AM-12.01B	Removable Media and Endpoint Devices	Based on a risk assessment (cf. OIS-07), the cloud service provider designs, implements and maintains controls for endpoint devices and removable storage media regarding the following aspects:	Functional	Intersects With	Endpoint Device Management (EDM)	END-02	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	3		END-01
AM-12.01B.1	Removable Media and Endpoint Devices	Except for system administrative tasks for which no other method is available, the use of removable media is forbidden;	Functional	Intersects With	Digital Media Use Restrictions	DCH-19	Mechanisms exist to restrict the use of types of digital media on systems or system components.	8		DCH-10
AM-12.01B.2	Removable Media and Endpoint Devices	Removable media is used for dedicated, specific purposes only;	Functional	Intersects With	Digital Media Use Restrictions	DCH-19	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5		DCH-10
AM-12.01B.2	Removable Media and Endpoint Devices	Removable media is used for dedicated, specific purposes only;	Functional	Intersects With	Removable Media Security	DCH-21	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	3		DCH-12

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
AM-12.01B.3	Removable Media and Endpoint Devices	Storage encryption is enabled on managed endpoints and removable storage media (except those used for unavoidable system administration actions) to protect information from unauthorised disclosure;	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	5		CRY-05
AM-12.01B.3	Removable Media and Endpoint Devices	Storage encryption is enabled on managed endpoints and removable storage media (except those used for unavoidable system administration actions) to protect information from unauthorised disclosure;	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-04	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	3		MDM-03
AM-12.01B.4	Removable Media and Endpoint Devices	Managed endpoints are configured with anti-malware detection and prevention technology and services;	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	8		END-04
AM-12.01B.5	Removable Media and Endpoint Devices	Self-execution from removable storage is disabled and storage media is scanned before use on the cloud service provider's systems;	Functional	Intersects With	Removable Media Security	DCH-21	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5		DCH-12
AM-12.01B.5	Removable Media and Endpoint Devices	Self-execution from removable storage is disabled and storage media is scanned before use on the cloud service provider's systems;	Functional	Intersects With	Heuristic / Nonsignature-Based Malware Detection	END-04.2	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	3		END-04.4
AM-12.01B.6	Removable Media and Endpoint Devices	Measures are to be taken by users to protect mobile endpoints and removable storage in transit and in storage;	Functional	Intersects With	Media Storage	DCH-13	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	3		DCH-06
AM-12.01B.6	Removable Media and Endpoint Devices	Measures are to be taken by users to protect mobile endpoints and removable storage in transit and in storage;	Functional	Intersects With	Media Transportation	DCH-16	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security	3		DCH-07
AM-12.01B.7	Removable Media and Endpoint Devices	Protection in terms of confidentiality and integrity of any equipment containing cloud service customer data during the transfer off-site for disposal is equivalent to that on the site;	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-22	Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent: (1) Data recovery; and (2) Components from being resold, redistributed and/or reused through unauthorized channels.	3		AST-09
AM-12.01B.7	Removable Media and Endpoint Devices	Protection in terms of confidentiality and integrity of any equipment containing cloud service customer data during the transfer off-site for disposal is equivalent to that on the site;	Functional	Intersects With	Media Transportation	DCH-16	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security	5		DCH-07
AM-12.01B.8	Removable Media and Endpoint Devices	Cloud service customer data and cloud service derived data stored on shareable equipment is encrypted in accordance with CRY-05 or destroyed using a secure deletion mechanism before the equipment is shared with a third party;	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	3		CRY-05
AM-12.01B.8	Removable Media and Endpoint Devices	Cloud service customer data and cloud service derived data stored on shareable equipment is encrypted in accordance with CRY-05 or destroyed using a secure deletion mechanism before the equipment is shared with a third party;	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5		DCH-09
AM-12.01B.9	Removable Media and Endpoint Devices	Users are to use mobile endpoints and removable storage in a secure manner, this includes for example not leaving media openly accessible in public spaces, using screen locks and screen privacy films; and	Functional	Intersects With	Unattended End-User Equipment	AST-20	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and	5		AST-06
AM-12.01B.9	Removable Media and Endpoint Devices	Users are to use mobile endpoints and removable storage in a secure manner, this includes for example not leaving media openly accessible in public spaces, using screen locks and screen privacy films; and	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3		SAT-02
AM-12.01B.10	Removable Media and Endpoint Devices	Measures for maintaining proper security of third party endpoints with access to organisational assets are to be defined.	Functional	Intersects With	Use of Third-Party Devices	AST-26	Mechanisms exist to reduce the risk associated with third-party assets that are connected to the network from: (1) Harming organizational assets; (2) Accessing unauthorized resources within the organization; and/or (3) Exfiltrating organizational data.	5		AST-13
AM-12.01B.10	Removable Media and Endpoint Devices	Measures for maintaining proper security of third party endpoints with access to organisational assets are to be defined.	Functional	Intersects With	Documented Endpoint Security Protection Measures	END-06	Mechanisms exist to document endpoint protection-related Technology Assets, Applications and/or Services (TAAS)	5		END-04.2
AM-12.01B.10	Removable Media and Endpoint Devices	Measures for maintaining proper security of third party endpoints with access to organisational assets are to be defined.	Functional	Intersects With	Third-Party Personnel Security	TPM-13	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	3		TPM-06
AM-12.01AC	Removable Media and Endpoint Devices	Policies and procedures for endpoint devices and removable storage media furthermore contain the following aspects:	Functional	Intersects With	Endpoint Device Management (EDM)	END-02	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	3		END-01
AM-12.01AC.1	Removable Media and Endpoint Devices	Managed endpoints are configured with appropriate software firewalls;	Functional	Intersects With	Software Firewall	END-07	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all endpoint devices, where technically feasible.	5		END-05
AM-12.01AC.2	Removable Media and Endpoint Devices	Managed endpoints are configured with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment (cf. OIS-07);	Functional	Intersects With	Data Loss Prevention (DLP)	DCH-40	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and	5		NET-17
AM-12.01AC.3	Removable Media and Endpoint Devices	Remote geo-location capabilities are enabled for all managed mobile endpoints; and	Functional	Intersects With	Automated Location Tracking	AST-09.3	Mechanisms exist to track the geographic location of system components.	5		AST-02.10
AM-12.01AC.3	Removable Media and Endpoint Devices	Remote geo-location capabilities are enabled for all managed mobile endpoints; and	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	3		MDM-01
AM-12.01AC.4	Removable Media and Endpoint Devices	Define, implement and evaluate processes, procedures and technical safeguards to enable the deletion of company data remotely on managed endpoint devices.	Functional	Intersects With	Remote Purging	MDM-09	Mechanisms exist to remotely purge selected information from mobile devices.	8		MDM-05
5.5	Physical Security (PS)	Objective: Prevent unauthorised physical access and protect against theft, damage, loss and outage of operations.	Functional	No Relationship	N/A	N/A	N/A	0		
PS-01.01B	Physical Security and Environmental Control Requirements	The cloud service provider defines and documents at least two security areas, with at least one sensitive area and one public area. A sensitive area covers the buildings and premises in which sensitive activities take place, such as hosting the system components used for providing the cloud service. A public area covers all buildings and premises not otherwise covered by a security area.	Functional	Intersects With	Zone-Based Physical Security	PES-04	Mechanisms exist to implement a zone-based approach to physical security.	8		PES-01.2
PS-01.02B	Physical Security and Environmental Control Requirements	Security requirements for premises and buildings related to the cloud service provided are based on the security objectives of the information security policy, protection needs identified for the cloud service and a risk assessment regarding physical and environmental security. The security requirements are documented, communicated and provided in a policy or framework according to SP-01.	Functional	Intersects With	Physical & Environmental Security Policy	PES-01	Mechanisms exist to establish a formal, documented physical and environmental security policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and	5		
PS-01.02B	Physical Security and Environmental Control Requirements	Security requirements for premises and buildings related to the cloud service provided are based on the security objectives of the information security policy, protection needs identified for the cloud service and a risk assessment regarding physical and environmental security. The security requirements are documented, communicated and provided in a policy or framework according to SP-01.	Functional	Intersects With	Physical Security Plan (PSP)	PES-03	Mechanisms exist to document a Physical Security Plan (PSP), or similar document, to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.	8		PES-01.1
PS-01.02B	Physical Security and Environmental Control Requirements	Security requirements for premises and buildings related to the cloud service provided are based on the security objectives of the information security policy, protection needs identified for the cloud service and a risk assessment regarding physical and environmental security. The security requirements are documented, communicated and provided in a policy or framework according to SP-01.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
PS-01.03B	Physical Security and Environmental Control Requirements	Security requirements for data centres are based on criteria in accordance with established rules of technology and the criteria PS-02 to PS-07. They are suitable for addressing the following risks in accordance with the applicable legal and contractual requirements:	Functional	Intersects With	Physical Security Plan (PSP)	PES-03	Mechanisms exist to document a Physical Security Plan (PSP), or similar document, to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.	5		PES-01.1
PS-01.03B.1	Physical Security and Environmental Control Requirements	Faults in planning;	Functional	Intersects With	Physical Security Plan (PSP)	PES-03	Mechanisms exist to document a Physical Security Plan (PSP), or similar document, to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.	3		PES-01.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
PS-01.03B.2	Physical Security and Environmental Control Requirements	Unauthorised access (including access to the premises by drones);	Functional	Intersects With	Physical Access Control	PES-08	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5		PES-03
PS-01.03B.3	Physical Security and Environmental Control Requirements	Insufficient surveillance;	Functional	Intersects With	Monitoring Physical Access	PES-13	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5		PES-05
PS-01.03B.4	Physical Security and Environmental Control Requirements	Lightning and overvoltage (aligned with the internationally harmonised standards of IEC 62305);	Functional	Intersects With	Automatic Voltage Controls	PES-20.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	3		PES-07.1
PS-01.03B.5	Physical Security and Environmental Control Requirements	Fire and smoke;	Functional	Intersects With	Fire Protection	PES-26	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	5		PES-08
PS-01.03B.6	Physical Security and Environmental Control Requirements	Unwanted water;	Functional	Intersects With	Water Damage Protection	PES-24	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key	5		PES-07.5
PS-01.03B.7	Physical Security and Environmental Control Requirements	Failures and/or unavailable telecommunications;	Functional	Intersects With	Supporting Utilities	PES-20	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5		PES-07
PS-01.03B.8	Physical Security and Environmental Control Requirements	Power failure; and	Functional	Intersects With	Emergency Power	PES-22	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5		PES-07.3
PS-01.03B.9	Physical Security and Environmental Control Requirements	Insufficient heating, ventilation, airconditioning (HVAC) and filtration.	Functional	Intersects With	Temperature & Humidity Controls Monitoring	PES-29	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	5		PES-09
PS-01.04B	Physical Security and Environmental Control Requirements	The maximum tolerable downtimes of utility facilities are suitable for meeting the availability requirements contained in the service level agreement.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
PS-01.04B	Physical Security and Environmental Control Requirements	The maximum tolerable downtimes of utility facilities are suitable for meeting the availability requirements contained in the service level agreement.	Functional	Intersects With	Supporting Utilities	PES-20	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	3		PES-07
PS-01.05B	Physical Security and Environmental Control Requirements	If the cloud service provider operates the cloud service in data centres operated by service organisations, the document describes:	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-11	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	3		TPM-05.4
PS-01.05B.1	Physical Security and Environmental Control Requirements	The complementary subservice organisation controls (CSOC) expected at the service organisations; and	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
PS-01.05B.2	Physical Security and Environmental Control Requirements	The measures for monitoring the design and operation of controls at the service organisations with respect to these CSOC (cf. SSO-05).	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
PS-01.06B	Physical Security and Environmental Control Requirements	If the cloud service provider operates the cloud service in data centres operated by service organisations, the cloud service provider performs a verification of the implementation of suitable CSOC in accordance with the criteria for controlling and monitoring service organisations (cf. SSO-05).	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
PS-01.01AC	Physical Security and Environmental Control Requirements	The security requirements include time constraints for self-sufficient operation in the event of exceptional events (e.g. prolonged power outage, heat waves, low water in cold river water supply) and maximum tolerable utility downtime.	Functional	Intersects With	Supporting Utilities	PES-20	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	3		PES-07
PS-01.02AC	Physical Security and Environmental Control Requirements	The security requirements include time limits in order to provide self-sufficient operation of a location for at least 72 hours in the event of a failure of the external power supply, or until all services are transferred to another location.	Functional	Intersects With	Emergency Power	PES-22	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	3		PES-07.3
PS-01.03AC	Physical Security and Environmental Control Requirements	The security requirements for a self-sufficient operation during a heat period are based on the highest outside temperatures that can reasonably be estimated to occur at the locations of the premises and buildings within the lifespan of the cooling supply system. The cloud service provider determines these temperatures with an appropriate safety margin.	Functional	Intersects With	Temperature & Humidity Controls Monitoring	PES-29	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	3		PES-09
PS-01.04AC	Physical Security and Environmental Control Requirements	The security requirements stipulate that the permissible operating and environmental parameters of the cooling supply system shall also be maintained on at least five consecutive days with these outside temperatures including the safety margin (cf. PS-06).	Functional	Intersects With	Temperature & Humidity Controls Monitoring	PES-29	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	3		PES-09
PS-01.05AC	Physical Security and Environmental Control Requirements	The security requirements take into account that if water is taken from a body of water (e.g., river or lake) for air conditioning, it is determined at which water levels and water temperatures the air conditioning can be maintained for how long.	Functional	Intersects With	Temperature & Humidity Controls Monitoring	PES-29	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	3		PES-09
PS-02.01B	Redundancy Model	The cloud service is provided from at least two locations. The locations meet the security requirements of the cloud service provider (cf. PS-01) and are located in an adequate distance to each other to achieve operational redundancy and resilience.	Functional	Intersects With	Alternate Processing Site	BCD-13	Mechanisms exist to establish an alternate processing site that provides processing capability and security measures equivalent to that of the primary site.	5		BCD-09
PS-02.01B	Redundancy Model	The cloud service is provided from at least two locations. The locations meet the security requirements of the cloud service provider (cf. PS-01) and are located in an adequate distance to each other to achieve operational redundancy and resilience.	Functional	Intersects With	Physical Security Plan (PSP)	PES-03	Mechanisms exist to document a Physical Security Plan (PSP), or similar document, to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.	3		PES-01.1
PS-02.02B	Redundancy Model	Operational redundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
PS-02.02B	Redundancy Model	Operational redundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met.	Functional	Intersects With	Alternate Processing Site	BCD-13	Mechanisms exist to establish an alternate processing site that provides processing capability and security measures equivalent to that of the	3		BCD-09
PS-02.03B	Redundancy Model	The effectiveness of the redundancy is checked at least annually by suitable tests and exercises (cf. BCM-04).	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
PS-02.01AS	Redundancy Model	PS-02.01AS, sharpening PS-02.01B The cloud service is provided from more than two locations. The locations meet the security requirements of the cloud service provider (cf. PS-01) and are located sufficiently far apart to achieve georedundancy and resilience. If two locations fail at the same time, at least one third location is still available to prevent a total service	Functional	Intersects With	Alternate Processing Site	BCD-13	Mechanisms exist to establish an alternate processing site that provides processing capability and security measures equivalent to that of the primary site.	3		BCD-09
PS-02.02AS	Redundancy Model	PS-02.02AS, sharpening PS-02.02B The georedundancy is designed in a way that ensures that the availability requirements specified in the service level agreement are met.	Functional	Intersects With	Alternate Processing Site	BCD-13	Mechanisms exist to establish an alternate processing site that provides processing capability and security measures equivalent to that of the primary site.	3		BCD-09
PS-03.01B	Perimeter Protection	The structural shell of premises and buildings related to the cloud service provided are physically solid and protected by adequate security measures that meet the security requirements of the cloud service provider (cf. PS-01).	Functional	Intersects With	Controlled Ingress & Egress Points	PES-09	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	5		PES-03.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
PS-03.01B	Perimeter Protection	The structural shell of premises and buildings related to the cloud service provided are physically solid and protected by adequate security measures that meet the security requirements of the cloud service provider (cf. PS-01).	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-10	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5		PES-04
PS-03.02B	Perimeter Protection	The security measures are designed to detect and prevent unauthorised access so that the information security of the cloud service is not compromised.	Functional	Intersects With	Physical Access Control	PES-08	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5		PES-03
PS-03.02B	Perimeter Protection	The security measures are designed to detect and prevent unauthorised access so that the information security of the cloud service is not compromised.	Functional	Intersects With	Monitoring Physical Access	PES-13	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5		PES-05
PS-03.03B	Perimeter Protection	The outer doors, windows and other construction elements exhibit an appropriate security level so that their combined resistance time withstand a break-in attempt for at least ten minutes in total. This time period applies from the moment an external intruder is detected (e.g. by perimeter surveillance).	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-10	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	3		PES-04
PS-03.04B	Perimeter Protection	The surrounding wall constructions as well as the locking mechanisms meet the associated requirements.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-10	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	3		PES-04
PS-03.05B	Perimeter Protection	If the construction elements as a whole do not fully meet the associated requirements, compensating controls are implemented to restore the appropriate security level.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2
PS-03.06B	Perimeter Protection	Data centre personnel are trained on how to respond effectively to unauthorised ingress or egress attempts.	Functional	Intersects With	Monitoring Physical Access	PES-13	Physical access control mechanisms exist to monitor for, detect and respond to physical security	3		PES-05
PS-03.06B	Perimeter Protection	Data centre personnel are trained on how to respond effectively to unauthorised ingress or egress attempts.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03
PS-03.01AC	Perimeter Protection	The security measures installed at the site include permanently present security personnel (at least two individuals), video surveillance and anti-burglary systems.	Functional	Intersects With	Physical Access Control	PES-08	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	3		PES-03
PS-03.01AC	Perimeter Protection	The security measures installed at the site include permanently present security personnel (at least two individuals), video surveillance and anti-burglary systems.	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-13.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5		PES-05.1
PS-04.01B	Physical Site Access Control	Preventive and detective physical access controls in premises and buildings related to the cloud service provided are implemented. They are in accordance with the cloud service provider's security requirements (cf. PS-01) and based on the principles defined in IAM-01 to prevent unauthorised access. They are documented and communicated in a policy or framework in accordance with SP-01 and include the following aspects:	Functional	Intersects With	Physical Access Authorizations	PES-06	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5		PES-02
PS-04.01B	Physical Site Access Control	Preventive and detective physical access controls in premises and buildings related to the cloud service provided are implemented. They are in accordance with the cloud service provider's security requirements (cf. PS-01) and based on the principles defined in IAM-01 to prevent unauthorised access. They are documented and communicated in a policy or framework in accordance with SP-01 and include the following aspects:	Functional	Intersects With	Physical Access Control	PES-08	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	8		PES-03
PS-04.01B.1	Physical Site Access Control	Specified procedure for the granting and modifying of user accounts and access rights (cf. IAM-02) based on the 'least-privilege-principle' and the 'need-to-know-principle';	Functional	Intersects With	Physical Access Authorizations	PES-06	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5		PES-02
PS-04.01B.1	Physical Site Access Control	Specified procedure for the granting and modifying of user accounts and access rights (cf. IAM-02) based on the 'least-privilege-principle' and the 'need-to-know-principle';	Functional	Intersects With	Role-Based Physical Access	PES-07	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	3		PES-02.1
PS-04.01B.2	Physical Site Access Control	Revocation of access authorisations if they have not been used for a period of two months. Exceptions are only made for well-founded individual cases and follow a defined exception process according to SP-03;	Functional	Intersects With	Physical Access Authorizations	PES-06	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	3		PES-02
PS-04.01B.3	Physical Site Access Control	Authentication with at least one factor for access to any non-public area;	Functional	Intersects With	Physical Access Control	PES-08	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5		PES-03
PS-04.01B.4	Physical Site Access Control	Multi-factor authentication for access to areas hosting system components that process cloud service customer data;	Functional	Intersects With	Access To Critical Systems	PES-12	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive and/or regulated data, in addition to the physical access controls for the facility.	5		PES-03.4
PS-04.01B.5	Physical Site Access Control	Existence and nature of access logging that enables the cloud service provider, in the sense of an effectiveness audit, to check whether only defined personnel have entered the premises and buildings related to the cloud service provided;	Functional	Intersects With	Physical Access Logs	PES-09.1	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	8		PES-03.3
PS-04.01B.6	Physical Site Access Control	Physical access control exceptions applicable in case of emergency, including an analysis procedure following every use of these exceptions; and	Functional	Intersects With	Physical Access Control	PES-08	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	3		PES-03
PS-04.01B.7	Physical Site Access Control	For visitors and external personnel, measures that ensure identification and tracking of every individual such that their activities are traceable and - in case of activities that infringe information security - stoppable in an appropriate reaction time. These measures are appropriate and proportional to the sensitivity of the zone the visitors or external personnel are in. The appropriate reaction time frame is determined based on a risk assessment (cf. OIS-07).	Functional	Intersects With	Visitor Control	PES-14	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5		PES-06
PS-04.01B.7	Physical Site Access Control	For visitors and external personnel, measures that ensure identification and tracking of every individual such that their activities are traceable and - in case of activities that infringe information security - stoppable in an appropriate reaction time. These measures are appropriate and proportional to the sensitivity of the zone the visitors or external personnel are in. The appropriate reaction time frame is determined based on a risk assessment (cf. OIS-07).	Functional	Intersects With	Restrict Unescorted Access	PES-14.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5		PES-06.3
PS-04.02B	Physical Site Access Control	The cloud service provider displays a warning at the entrance of each applicable non-public area regarding its limits and access conditions.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-10	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	3		PES-04
PS-04.03B	Physical Site Access Control	Physical access control to the site is managed by an electronic access control system that supports authentication, authorisation, and logging of entry and exit events.	Functional	Intersects With	Physical Access Control	PES-08	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5		PES-03
PS-04.03B	Physical Site Access Control	Physical access control to the site is managed by an electronic access control system that supports authentication, authorisation, and logging of entry and exit events.	Functional	Intersects With	Physical Access Logs	PES-09.1	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	3		PES-03.3

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
PS-05.01B	Protection against Threats from Outside and from the Environment	Premises and buildings related to the cloud service provided are protected from fire, smoke, lightning and unwanted water by structural, technical and organisational measures that meet the security requirements of the cloud service provider (cf. PS-01).	Functional	Intersects With	Physical & Environmental Protections	PES-02	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5		PES-01
PS-05.01B	Protection against Threats from Outside and from the Environment	Premises and buildings related to the cloud service provided are protected from fire, smoke, lightning and unwanted water by structural, technical and organisational measures that meet the security requirements of the cloud service provider (cf. PS-01).	Functional	Intersects With	Water Damage Protection	PES-24	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key	3		PES-07.5
PS-05.01B	Protection against Threats from Outside and from the Environment	Premises and buildings related to the cloud service provided are protected from fire, smoke, lightning and unwanted water by structural, technical and organisational measures that meet the security requirements of the cloud service provider (cf. PS-01).	Functional	Intersects With	Fire Protection	PES-26	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	5		PES-08
PS-05.02B	Protection against Threats from Outside and from the Environment	Structural Measures include the following aspects:	Functional	Intersects With	Physical & Environmental Protections	PES-02	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	3		PES-01
PS-05.02B.1	Protection against Threats from Outside and from the Environment	Establishment of fire sections with a fire resistance duration of at least 90 minutes for all structural parts, or alternatively, equivalent organisational and technical measures that ensure the same level of protection standard as 90-minutes fire-resistant structural parts or establishment of compensating measures for containing fires and maintaining operational capability. If compensating measures are taken into account, the fire resistance of structural parts has to be at least 60 minutes;	Functional	Intersects With	Fire Protection	PES-26	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	3		PES-08
PS-05.02B.2	Protection against Threats from Outside and from the Environment	Effective implementation of measures to protect against lightning and overvoltage damage; and	Functional	Intersects With	Automatic Voltage Controls	PES-20.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	3		PES-07.1
PS-05.02B.3	Protection against Threats from Outside and from the Environment	Effective implementation of measures to protect against flooding, unless critical facilities are located significantly above the highest flood level at the location of the cloud data centre. Additionally, appropriate measures to mitigate the effects of heavy rain are implemented, unless critical facilities are located significantly above the backwater level at the location of the cloud data centre.	Functional	Intersects With	Water Damage Protection	PES-24	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	5		PES-07.5
PS-05.03B	Protection against Threats from Outside and from the Environment	Technical Measures include the following aspects:	Functional	Intersects With	Fire Protection	PES-26	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	3		PES-08
PS-05.03B.1	Protection against Threats from Outside and from the Environment	Early fire detection with automatic voltage release. The monitored areas are sufficiently fragmented to ensure that the prevention of the spread of incipient fires is proportionate to the maintenance of the availability of the cloud service provided;	Functional	Intersects With	Fire Detection Devices	PES-27	Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire.	5		PES-08.1
PS-05.03B.2	Protection against Threats from Outside and from the Environment	Extinguishing system or oxygen reduction; and	Functional	Intersects With	Fire Suppression Devices	PES-28	Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency responders.	5		PES-08.2
PS-05.03B.2	Protection against Threats from Outside and from the Environment	Extinguishing system or oxygen reduction; and	Functional	Intersects With	Automatic Fire Suppression	PES-28.1	Facility security mechanisms exist to employ an automatic fire suppression capability for critical systems when the facility is not staffed on a continuous basis.	3		PES-08.3
PS-05.03B.3	Protection against Threats from Outside and from the Environment	Fire alarm system with reporting to the local fire department.	Functional	Intersects With	Fire Detection Devices	PES-27	Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire.	5		PES-08.1
PS-05.04B	Protection against Threats from Outside and from the Environment	Organisational Measures include the following aspects:	Functional	Intersects With	Fire Protection	PES-26	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	3		PES-08
PS-05.04B.1	Protection against Threats from Outside and from the Environment	Regular fire protection inspections to check compliance with fire protection requirements; and	Functional	Intersects With	Fire Protection	PES-26	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	3		PES-08
PS-05.04B.2	Protection against Threats from Outside and from the Environment	Regular fire protection exercises.	Functional	Intersects With	Fire Protection	PES-26	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	3		PES-08
PS-06.01B	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Measures to prevent the failure of the technical supply facilities required for the operation of system components with which cloud service customer data is processed and to protect equipment containing cloud service customer data, are documented and set up in accordance with the security requirements of the cloud service provider (cf. PS-01) with respect to the following aspects:	Functional	Intersects With	Supporting Utilities	PES-20	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	8		PES-07
PS-06.01B.1	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Operational redundancy (N+1) in power and cooling supply;	Functional	Intersects With	Supporting Utilities	PES-20	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5		PES-07
PS-06.01B.1	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Operational redundancy (N+1) in power and cooling supply;	Functional	Intersects With	Redundant Cabling	PES-25	Mechanisms exist to employ redundant power cabling paths that are physically separated to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.	3		PES-07.7
PS-06.01B.2	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Use of appropriately sized uninterruptible power supplies (UPSes) and emergency power supplies (EPSes), designed to ensure that all data remains undamaged in the event of a power failure. The functionality of UPSes and EPSes is checked at least annually by suitable tests and exercises (cf. BCM-04);	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	3		BCD-04
PS-06.01B.2	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Use of appropriately sized uninterruptible power supplies (UPSes) and emergency power supplies (EPSes), designed to ensure that all data remains undamaged in the event of a power failure. The functionality of UPSes and EPSes is checked at least annually by suitable tests and exercises (cf. BCM-04);	Functional	Intersects With	Emergency Power	PES-22	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5		PES-07.3
PS-06.01B.3	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Maintenance (servicing, inspection, repair) of the utilities in accordance with the manufacturer's recommendations; and	Functional	Intersects With	Controlled Maintenance	MNT-03	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	5		MNT-02
PS-06.01B.4	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Protection of power supply and telecommunications lines against interruption, interference, damage and eavesdropping.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1
PS-06.02B	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Uninterruptible Power Supplies (UPSes) and Emergency Power Supplies (EPSes) are implemented to comply with the availability requirements defined in the Service Level Agreement.	Functional	Intersects With	Emergency Power	PES-22	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5		PES-07.3
PS-06.03B	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	The protection of power supply and telecommunications lines is checked regularly, but at least every two years as well as in case of suspected manipulation, by qualified personnel regarding the following aspects:	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	5		PES-12.1
PS-06.03B.1	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Traces of violent attempts to open closed distributors;	Functional	Intersects With	Physical Tampering Detection	AST-29.1	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	3		AST-08

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
PS-06.03B.1	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Traces of violent attempts to open closed distributors;	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	3		PES-12.1
PS-06.03B.2	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Up-to-dateness of the documentation within the distributor;	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	3		PES-12.1
PS-06.03B.3	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Conformity of the actual wiring and patching with the documentation;	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	3		PES-12.1
PS-06.03B.4	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	The short-circuits and earthing of unneeded cables and wires are intact; and	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	3		PES-12.1
PS-06.03B.5	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Impermissible installations and modifications.	Functional	Intersects With	Physical Tampering Detection	AST-29.1	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	3		AST-08
PS-06.03B.5	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	Impermissible installations and modifications.	Functional	Intersects With	Transmission Medium Security	PES-16.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	3		PES-12.1
PS-06.01AC	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	The cooling supply system is designed in such a way that the permissible operating and environmental parameters are also ensured on at least five consecutive days with the highest outside temperatures that can reasonably be estimated to occur at the locations of the premises and buildings within the lifespan of the cooling supply system, with an appropriate safety margin.	Functional	Intersects With	Temperature & Humidity Controls Monitoring	PES-29	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	3		PES-09
PS-06.02AC	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	The connection to the telecommunications network is designed with sufficient redundancy so that the failure of a telecommunications network does not impair the security or performance of the cloud service provider.	Functional	Intersects With	Alternate Communications Channels	BCD-06.1	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable during a designated crisis situation.	3		BCD-10.4
PS-06.02AC	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	The connection to the telecommunications network is designed with sufficient redundancy so that the failure of a telecommunications network does not impair the security or performance of the cloud service provider.	Functional	Intersects With	Redundant Cabling	PES-25	Mechanisms exist to employ redundant power cabling paths that are physically separated to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.	3		PES-07.7
PS-06.03AC	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	The cloud service provider implements measures to ensure the compatibility of the conditions for installation, maintenance and servicing of the related technical equipment (e.g., electrical power, air conditioning, fire protection) with the cloud service's availability and security requirements.	Functional	Intersects With	Controlled Maintenance	MNT-03	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	3		MNT-02
PS-06.03AC	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	The cloud service provider implements measures to ensure the compatibility of the conditions for installation, maintenance and servicing of the related technical equipment (e.g., electrical power, air conditioning, fire protection) with the cloud service's availability and security requirements.	Functional	Intersects With	Equipment Siting & Protection	PES-16	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	3		PES-12
PS-06.04AC	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	The cloud service provider ensures that maintenance agreements for equipment used for the hosting of the cloud service enable the timely installation of security updates on this equipment.	Functional	Intersects With	Controlled Maintenance	MNT-03	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	3		MNT-02
PS-06.04AC	Protection against Interruptions caused by Power Failures and similar Risks to Supply Facilities	The cloud service provider ensures that maintenance agreements for equipment used for the hosting of the cloud service enable the timely installation of security updates on this equipment.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
PS-07.01B	Surveillance of Operational and Environmental Parameters	The operating parameters of the technical utilities (cf. PS-06) and the environmental parameters of the premises and buildings related to the cloud service provided are monitored and controlled in accordance with the security requirements of the cloud service provider (cf. PS-01).	Functional	Intersects With	Monitoring Physical Access	PES-13	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	3		PES-05
PS-07.01B	Surveillance of Operational and Environmental Parameters	The operating parameters of the technical utilities (cf. PS-06) and the environmental parameters of the premises and buildings related to the cloud service provided are monitored and controlled in accordance with the security requirements of the cloud service provider (cf. PS-01).	Functional	Intersects With	Temperature & Humidity Controls Monitoring	PES-29	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	5		PES-09
PS-07.02B	Surveillance of Operational and Environmental Parameters	When the permitted control range is exceeded, the responsible departments at the cloud service provider are automatically informed in order to timely initiate the necessary measures for return to the control range.	Functional	Intersects With	Temperature & Humidity Controls Alerting	PES-29.1	Facility security mechanisms exist to trigger an alarm or notification of temperature and humidity changes that are potentially harmful to personnel or equipment.	8		PES-09.1
PS-08.01B	Workplace Security Requirements	Based on a risk assessment according to OIS-07, security requirements for office environments are documented, communicated and provided in accordance with SP-01. The security requirements for rented offices take into account proportionality and appropriateness, potentially being less extensive than those in own office environments. These security requirements encompass various aspects for a safe and secure working environment, including at least:	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-10	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5		PES-04
PS-08.01B	Workplace Security Requirements	Based on a risk assessment according to OIS-07, security requirements for office environments are documented, communicated and provided in accordance with SP-01. The security requirements for rented offices take into account proportionality and appropriateness, potentially being less extensive than those in own office environments. These security requirements encompass various aspects for a safe and secure working environment, including at least:	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
PS-08.01B.1	Workplace Security Requirements	Physical access controls, such as key cards and biometric scanners, for office buildings;	Functional	Intersects With	Physical Access Control	PES-08	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5		PES-03
PS-08.01B.2	Workplace Security Requirements	Use of screen locks and privacy screens for workstations;	Functional	Intersects With	Unattended End-User Equipment	AST-20	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and	5		AST-06
PS-08.01B.3	Workplace Security Requirements	No openly visible confidential data at temporarily unattended workstations;	Functional	Intersects With	Unattended End-User Equipment	AST-20	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and	5		AST-06
PS-08.01B.4	Workplace Security Requirements	Disposal of all company documents that are no longer required within the company premise;	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-08 DCH-21
PS-08.01B.5	Workplace Security Requirements	Prohibition of the use of third party equipment; and	Functional	Intersects With	Use of Third-Party Devices	AST-26	Mechanisms exist to reduce the risk associated with third-party assets that are connected to the network from: (1) Harming organizational assets; (2) Accessing unauthorized resources within the organization; and/or (3) Exfiltrating organizational data.	5		AST-13
PS-08.01B.6	Workplace Security Requirements	Securing the entrances of office premises with alarm systems and surveillance cameras.	Functional	Intersects With	Intrusion Alarms / Surveillance	PES-13.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance	5		PES-05.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
5.6	Operations (OPS)	Objective: Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures.	Functional	No Relationship	N/A	N/A	N/A	0		
OPS-01.01B	Capacity Management - Planning	The planning of capacities and resources (personnel and system components) follows an established procedure in order to avoid possible capacity restrictions.	Functional	Intersects With	Capacity & Performance Planning Policy	CAP-01	Mechanisms exist to establish a formal, documented capacity and performance planning policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected	5		
OPS-01.01B	Capacity Management - Planning	The planning of capacities and resources (personnel and system components) follows an established procedure in order to avoid possible capacity restrictions.	Functional	Intersects With	Capacity & Performance Management	CAP-02	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5		CAP-01
OPS-01.01B	Capacity Management - Planning	The planning of capacities and resources (personnel and system components) follows an established procedure in order to avoid possible capacity restrictions.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	8		CAP-03
OPS-01.02B	Capacity Management - Planning	The procedures include forecasting future capacity requirements in order to identify usage trends and manage system overload.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5		CAP-03
OPS-01.03B	Capacity Management - Planning	The cloud service provider takes appropriate measures to ensure that they continue to meet the requirements agreed with cloud service customers for the provision of the cloud service in the event of capacity restrictions or outages regarding personnel and system components. This applies in particular to those relating to the dedicated use of system components, in accordance with the respective agreements.	Functional	Intersects With	Capacity & Performance Management	CAP-02	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5		CAP-01
OPS-01.03B	Capacity Management - Planning	The cloud service provider takes appropriate measures to ensure that they continue to meet the requirements agreed with cloud service customers for the provision of the cloud service in the event of capacity restrictions or outages regarding personnel and system components. This applies in particular to those relating to the dedicated use of system components, in accordance with the respective agreements.	Functional	Intersects With	Resource Priority	CAP-04	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	3		CAP-02
OPS-01.01AC	Capacity Management - Planning	The forecasts are considered in accordance with the service level agreement for planning and preparing the provisioning.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	3		CAP-03
OPS-02.01B	Capacity Management - Monitoring	Procedures and technical safeguards for the monitoring, provisioning and de-provisioning of cloud services are defined. The cloud service provider ensures that resources are delivered as contractually agreed with the customers. The cloud service provider ensures compliance with the service level agreements.	Functional	Intersects With	Capacity & Performance Management	CAP-02	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	5		CAP-01
OPS-02.01B	Capacity Management - Monitoring	Procedures and technical safeguards for the monitoring, provisioning and de-provisioning of cloud services are defined. The cloud service provider ensures that resources are delivered as contractually agreed with the customers. The cloud service provider ensures compliance with the service level agreements.	Functional	Intersects With	Performance Monitoring	CAP-05	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical Technology Assets, Applications and/or Services (TAAS).	5		CAP-04
OPS-02.02B	Capacity Management - Monitoring	Capacity restrictions that result in breaches of contractual obligations are to be reported to cloud service customers in accordance with OPS-24.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	3		IRO-10
OPS-02.01AC	Capacity Management - Monitoring	To monitor capacity and availability managed by the cloud service customer, the relevant information is available to the cloud service customer in a self-service portal.	Functional	Intersects With	Performance Monitoring	CAP-05	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical Technology Assets, Applications and/or Services (TAAS).	3		CAP-04
OPS-03.01B	Capacity Management - Controlling of Resources	Depending on the capabilities of the respective service model, the cloud service customer can control and monitor the allocation of the system components assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient	Functional	Intersects With	Resource Priority	CAP-04	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	3		CAP-02
OPS-03.01B	Capacity Management - Controlling of Resources	Depending on the capabilities of the respective service model, the cloud service customer can control and monitor the allocation of the system components assigned to the customer for administration/use in order to avoid overcrowding of resources and to achieve sufficient performance.	Functional	Intersects With	Performance Monitoring	CAP-05	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical Technology Assets, Applications and/or Services (TAAS).	3		CAP-04
OPS-03.02B	Capacity Management - Controlling of Resources	If there are significant security changes, or planned significant security changes, in the system components provided as part of the cloud service and allocated by the cloud service customer, the cloud service provider informs the cloud service customer about them.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		CHG-05
OPS-04.01B	Protection Against Malware - Policies and Procedures	Policies and procedures with specifications for protection against malware are documented, communicated, and provided in accordance with SP-01 with respect to the following aspects:	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04
OPS-04.01B	Protection Against Malware - Policies and Procedures	Policies and procedures with specifications for protection against malware are documented, communicated, and provided in accordance with SP-01 with respect to the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
OPS-04.01B.1	Protection Against Malware - Policies and Procedures	Use of system-specific protection mechanisms;	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	3		END-04
OPS-04.01B.2	Protection Against Malware - Policies and Procedures	Operating protection programmes on system components under the responsibility of the cloud service provider;	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04
OPS-04.01B.3	Protection Against Malware - Policies and Procedures	Operation of protection programmes for personnel's terminal equipment; and	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04
OPS-04.01B.4	Protection Against Malware - Policies and Procedures	Operation of protection programmes on flows coming in over cloud service provider end-devices, as well as all other incoming flows.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	3		END-04
OPS-04.01B.4	Protection Against Malware - Policies and Procedures	Operation of protection programmes on flows coming in over cloud service provider end-devices, as well as all other incoming flows.	Functional	Intersects With	Phishing & Spam Protection	NET-40.2	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	3		END-08
OPS-05.01B	Protection Against Malware - Implementation	System components under the cloud service provider's responsibility that are used to operate the cloud service in the production environment are configured with malware protection according to the policies and procedures.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	8		END-04
OPS-05.02B	Protection Against Malware - Implementation	If protection programmes are set up with signature or behaviour-based malware detection and removal, these protection programmes are regularly updated with the latest malware definitions when they are available, at least on a daily basis.	Functional	Intersects With	Automatic Endpoint Protection Mechanism Updates	END-03.2	Automated mechanisms exist to update endpoint protection-related Technology Assets, Applications and/or Services (TAAS) when new releases are available, in accordance with organization-defined configuration and change management practices.	8		END-04.1
OPS-05.03B	Protection Against Malware - Implementation	The cloud service provider creates regular reports on the checks performed by the operated protection programmes, which are reviewed and analysed by authorised individuals, bodies or committees.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	3		END-04
OPS-05.03B	Protection Against Malware - Implementation	The cloud service provider creates regular reports on the checks performed by the operated protection programmes, which are reviewed and analysed by authorised individuals, bodies or committees.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	3		MON-06
OPS-05.02AS	Protection Against Malware - Implementation	OPS-05.02AS, sharpening OPS-05.02B If protection programmes are set up with signature and behaviour-based malware detection and removal, these protection programmes are regularly updated with the latest malware definitions when they are available, at the highest frequency that the vendor(s) offer(s) where applicable.	Functional	Intersects With	Automatic Endpoint Protection Mechanism Updates	END-03.2	Automated mechanisms exist to update endpoint protection-related Technology Assets, Applications and/or Services (TAAS) when new releases are available, in accordance with organization-defined configuration and change management practices.	8		END-04.1
OPS-05.01AC	Protection Against Malware - Implementation	Policies and procedures describe the technical measures taken to securely configure and monitor the management console (both the customer's self-service and the service provider's cloud administration) to protect it from malware.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-05.01AC	Protection Against Malware - Implementation	Policies and procedures describe the technical measures taken to securely configure and monitor the management console (both the customer's self-service and the service provider's cloud administration) to protect it from malware.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	3		END-04
OPS-05.02AC	Protection Against Malware - Implementation	The configuration of the protection mechanisms is monitored automatically.	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	5		CFG-06
OPS-05.03AC	Protection Against Malware - Implementation	Deviations from the specifications are automatically reported to the cloud service provider's subject matter experts so that they can be immediately assessed and the necessary measures taken.	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	3		CFG-06
OPS-05.03AC	Protection Against Malware - Implementation	Deviations from the specifications are automatically reported to the cloud service provider's subject matter experts so that they can be immediately assessed and the necessary measures taken.	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5		MON-01.4
OPS-06.01B	Data Backup and Recovery - Policies and Procedures	Policies and procedures for regular backup or replication and regular restore of cloud service customer data, cloud service derived data and cloud service provider data according to the sensitivity of the data are documented, communicated and provided in accordance with SP-01 regarding the following aspects:	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8		BCD-11
OPS-06.01B.1	Data Backup and Recovery - Policies and Procedures	The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud service customers and the cloud service provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO);	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-01.4
OPS-06.01B.1	Data Backup and Recovery - Policies and Procedures	The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud service customers and the cloud service provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO);	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-11
OPS-06.01B.2	Data Backup and Recovery - Policies and Procedures	Data is backed up in encrypted, state of the art form;	Functional	Intersects With	Encrypting Storage Media	CRY-07.1	Cryptographic mechanisms exist to protect the confidentiality and integrity of sensitive and/or regulated data residing on storage media.	5		CRY-05.1
OPS-06.01B.3	Data Backup and Recovery - Policies and Procedures	Secure storage, transfer, management and disposal of backup data;	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
OPS-06.01B.3	Data Backup and Recovery - Policies and Procedures	Secure storage, transfer, management and disposal of backup data;	Functional	Intersects With	Media Storage	DCH-13	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	3		DCH-06
OPS-06.01B.4	Data Backup and Recovery - Policies and Procedures	Access to the backed-up data and the execution of restores is performed only by authorised persons;	Functional	Intersects With	Data Backup Access	BCD-30	Mechanisms exist to restrict access to data backups to those privileged users with assigned roles for data backup and recovery operations.	8		BCD-11.9
OPS-06.01B.5	Data Backup and Recovery - Policies and Procedures	Tests of data restore procedures by the cloud service provider (cf. OPS-08); and	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	5		BCD-11.1
OPS-06.01B.6	Data Backup and Recovery - Policies and Procedures	If part of the contractual agreement: Execution of actual data restore requests or restore tests initiated by the cloud service customer.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
OPS-06.01B.7	Data Backup and Recovery - Policies and Procedures	The policies and procedures include conditions for those parts of cloud service provider data that do not require a backup. For those parts of cloud service provider data, this subcriterion is not applicable.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
OPS-06.01AS	Data Backup and Recovery - Policies and Procedures	OPS-06.01AS, sharpening OPS-06.01B Policies and procedures for at least daily backup or replication and at least daily restore of cloud service customer data, cloud service derived data and cloud service provider data according to the sensitivity of the data are documented, communicated and provided in accordance with SP-01 regarding the following aspects:	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8		BCD-11
OPS-06.01AS.1	Data Backup and Recovery - Policies and Procedures	The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud service customers and the cloud service provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO);	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-01.4
OPS-06.01AS.1	Data Backup and Recovery - Policies and Procedures	The extent and frequency of data backups and the duration of data retention are consistent with the contractual agreements with the cloud service customers and the cloud service provider's operational continuity requirements for Recovery Time Objective (RTO) and Recovery Point Objective (RPO);	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-11
OPS-06.01AS.2	Data Backup and Recovery - Policies and Procedures	Data is backed up in encrypted, state of the art form;	Functional	Intersects With	Encrypting Storage Media	CRY-07.1	Cryptographic mechanisms exist to protect the confidentiality and integrity of sensitive and/or regulated data residing on storage media.	5		CRY-05.1
OPS-06.01AS.3	Data Backup and Recovery - Policies and Procedures	Secure storage, transfer, management and disposal of backup data;	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
OPS-06.01AS.3	Data Backup and Recovery - Policies and Procedures	Secure storage, transfer, management and disposal of backup data;	Functional	Intersects With	Media Storage	DCH-13	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	3		DCH-06
OPS-06.01AS.4	Data Backup and Recovery - Policies and Procedures	Access to the backed-up data and the execution of restores is performed only by authorised persons;	Functional	Intersects With	Data Backup Access	BCD-30	Mechanisms exist to restrict access to data backups to those privileged users with assigned roles for data backup and recovery operations.	8		BCD-11.9
OPS-06.01AS.5	Data Backup and Recovery - Policies and Procedures	Tests of data restore procedures by the cloud service provider (cf. OPS-08); and	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	5		BCD-11.1
OPS-06.01AS.6	Data Backup and Recovery - Policies and Procedures	If part of the contractual agreement: Execution of actual data restore requests or restore tests initiated by the cloud service customer.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-06.01AS.7	Data Backup and Recovery - Policies and Procedures	The policies and procedures include conditions for those parts of cloud service provider data that do not require a backup. For those parts of cloud service provider data, this subcriterion is not applicable.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
OPS-07.01B	Data Backup and Recovery - Monitoring	The execution of backups of cloud service customer data, cloud service derived data and cloud service provider data is monitored by technical and organisational measures documented and implemented in accordance with the policies and procedures for data backup and recovery (cf. OPS-06).	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-11
OPS-07.01B	Data Backup and Recovery - Monitoring	The execution of backups of cloud service customer data, cloud service derived data and cloud service provider data is monitored by technical and organisational measures documented and implemented in accordance with the policies and procedures for data backup and recovery (cf. OPS-06).	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
OPS-07.02B	Data Backup and Recovery - Monitoring	Incidents are investigated by qualified personnel and rectified timely to ensure compliance with contractual obligations to cloud service customers or the cloud service provider's business requirements regarding the scope and frequency of data backup and the duration of storage.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
OPS-07.02B	Data Backup and Recovery - Monitoring	Incidents are investigated by qualified personnel and rectified timely to ensure compliance with contractual obligations to cloud service customers or the cloud service provider's business requirements regarding the scope and frequency of data backup and the duration of storage.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	3		IRO-02
OPS-07.01AC	Data Backup and Recovery - Monitoring	The relevant logs or summarised results are available to the cloud service customer in a self-service portal for monitoring the data backup.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
OPS-08.01B	Data Backup and Recovery - Regular Testing	Restore procedures are tested regularly, at least annually. The tests include cloud service provider data and, if contractually agreed upon, cloud service customer data and cloud service derived data.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	8		BCD-11.1
OPS-08.02B	Data Backup and Recovery - Regular Testing	The tests allow an assessment as to whether the contractual agreements as well as the specifications for the maximum tolerable downtime (Recovery Time Objective, RTO) and the maximum permissible data loss (Recovery Point Objective, RPO) are adhered to (cf. BCM-02).	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-01.4
OPS-08.02B	Data Backup and Recovery - Regular Testing	The tests allow an assessment as to whether the contractual agreements as well as the specifications for the maximum tolerable downtime (Recovery Time Objective, RTO) and the maximum permissible data loss (Recovery Point Objective, RPO) are adhered to (cf. BCM-02).	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	5		BCD-11.1
OPS-08.03B	Data Backup and Recovery - Regular Testing	Cloud service customer data is only restored in environments that are subject to the same access restrictions as the production environment.	Functional	Intersects With	Data Backup Access	BCD-30	Mechanisms exist to restrict access to data backups to those privileged users with assigned roles for data backup and recovery operations.	5		BCD-11.9
OPS-08.04B	Data Backup and Recovery - Regular Testing	Performed restore tests are thoroughly documented. This also includes the documentation of the safe disposal of the restored data.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	3		BCD-11.1
OPS-08.04B	Data Backup and Recovery - Regular Testing	Performed restore tests are thoroughly documented. This also includes the documentation of the safe disposal of the restored data.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	3		DCH-09
OPS-08.05B	Data Backup and Recovery - Regular Testing	Deviations from the specifications are reported to the responsible personnel or system components so that these can timely assess the deviations and initiate the necessary actions.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	3		BCD-11.1
OPS-08.05B	Data Backup and Recovery - Regular Testing	Deviations from the specifications are reported to the responsible personnel or system components so that these can timely assess the deviations and initiate the necessary actions.	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	3		MON-01.4
OPS-08.01AC	Data Backup and Recovery - Regular Testing	At the customer's request, the cloud service provider informs the cloud service customer of the results of the restore tests.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	3		BCD-11.1
OPS-08.02AC	Data Backup and Recovery - Regular Testing	Restore tests are included in the cloud service provider's business continuity management.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
OPS-09.01B	Data Backup and Recovery - Storage	The cloud service provider transfers cloud service provider data and, if contractually agreed upon, cloud service customer data and cloud service derived data to be backed up to a remote location or transports these on backup media to a remote location.	Functional	Intersects With	Separate Storage for Critical Information	BCD-24.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	8		BCD-11.2
OPS-09.02B	Data Backup and Recovery - Storage	The protection needs resulting from the data classification of the original data (e.g., encryption, access control) are also applied to backups.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-11
OPS-09.02B	Data Backup and Recovery - Storage	The protection needs resulting from the data classification of the original data (e.g., encryption, access control) are also applied to backups.	Functional	Intersects With	Data Backup Modification and/or Destruction	BCD-33	Mechanisms exist to restrict access to modify and/or delete data backups to only those privileged users with assigned data backup and recovery operations	5		BCD-11.10
OPS-09.02B	Data Backup and Recovery - Storage	The protection needs resulting from the data classification of the original data (e.g., encryption, access control) are also applied to backups.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	3		DCH-02
OPS-09.03B	Data Backup and Recovery - Storage	If the data backup is transmitted to the remote location via a network, the data backup or the transmission of the data takes place in an encrypted form that corresponds to the state of the art (cf. CRY-04).	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
OPS-09.03B	Data Backup and Recovery - Storage	If the data backup is transmitted to the remote location via a network, the data backup or the transmission of the data takes place in an encrypted form that corresponds to the state of the art (cf. CRY-04).	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
OPS-09.04B	Data Backup and Recovery - Storage	The distance to the main site is chosen after sufficient consideration of the factors recovery times and impact of disasters on both sites.	Functional	Intersects With	Separation from Primary Processing Site	BCD-13.1	Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats.	5		BCD-09.1
OPS-09.05B	Data Backup and Recovery - Storage	The physical and environmental security measures at the remote site are equivalent to those at the main site.	Functional	Intersects With	Alternate Storage Site	BCD-12	Mechanisms exist to establish an alternate storage site that stores both the assets and necessary agreements needed for the recovery of Technology	5		BCD-08
OPS-09.05B	Data Backup and Recovery - Storage	The physical and environmental security measures at the remote site are equivalent to those at the main site.	Functional	Intersects With	Alternate Processing Site	BCD-13	Mechanisms exist to establish an alternate processing site that provides processing capability and security measures equivalent to that of the primary site.	5		BCD-09
OPS-10.01B	Logging and Monitoring - Policies and Procedures	The cloud service provider has established policies and procedures that govern the logging and monitoring of events on system components within its area of responsibility. These policies and procedures are documented, communicated and provided according to SP-01 with respect to the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-10.01B	Logging and Monitoring - Policies and Procedures	The cloud service provider has established policies and procedures that govern the logging and monitoring of events on system components within its area of responsibility. These policies and procedures are documented, communicated and provided according to SP-01 with respect to the following aspects:	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
OPS-10.01B.1	Logging and Monitoring - Policies and Procedures	Definition of events that could lead to a violation of the protection goals;	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5		MON-01.8
OPS-10.01B.1	Logging and Monitoring - Policies and Procedures	Definition of events that could lead to a violation of the protection goals;	Functional	Intersects With	Centralized Event Log & Security-Relevant Telemetry Review & Analysis	MON-05.1	Automated mechanisms exist to centrally collect, review and analyze event logs and security-relevant telemetry from multiple sources.	3		MON-02.2
OPS-10.01B.2	Logging and Monitoring - Policies and Procedures	Specifications for activating, stopping and pausing the various logs;	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
OPS-10.01B.3	Logging and Monitoring - Policies and Procedures	Information regarding the purpose and retention period of the logs;	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5		MON-10
OPS-10.01B.4	Logging and Monitoring - Policies and Procedures	Definition of roles, responsibilities and authorities for setting up and monitoring logging;	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	3		HRS-03
OPS-10.01B.4	Logging and Monitoring - Policies and Procedures	Definition of roles, responsibilities and authorities for setting up and monitoring logging;	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
OPS-10.01B.5	Logging and Monitoring - Policies and Procedures	Definition of log data allowed for transfer to cloud service customers and technical requirements of such a transfer;	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-07.1	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	5		CLD-06.2
OPS-10.01B.6	Logging and Monitoring - Policies and Procedures	Information regarding timestamps used in event creation;	Functional	Intersects With	Time Stamps	MON-11	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs and security-relevant telemetry.	5		MON-07
OPS-10.01B.7	Logging and Monitoring - Policies and Procedures	Time synchronisation of system components with at least one approved time source that the cloud service provider considers to be reliable based on defined criteria. If several time sources are used, they are consistent with each other. The time sources can also be synchronised to several external reliable sources, except when used for isolated networks; and	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-11.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5		MON-07.1
OPS-10.01B.8	Logging and Monitoring - Policies and Procedures	Compliance with legal and regulatory frameworks.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
OPS-11.01B	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	Policies and procedures for the secure handling of cloud service derived data and account data are documented, communicated and provided according to SP-01 with regard to at least the following aspects:	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	5		DCH-01
OPS-11.01B	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	Policies and procedures for the secure handling of cloud service derived data and account data are documented, communicated and provided according to SP-01 with regard to at least the following aspects:	Functional	Intersects With	Media & Data Retention	DCH-27	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	3		DCH-18
OPS-11.01B.1	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	Cloud service derived data and account data is collected and used solely to administer and operate the cloud service, including purposes related to the implementation of security controls;	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-30	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5		PRI-05
OPS-11.01B.2	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	No commercial use beyond the aforementioned purpose to administer and operate the cloud service;	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-30	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5		PRI-05
OPS-11.01B.3	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	Storage for a fixed period reasonably related to the purposes of the collection;	Functional	Intersects With	Media & Data Retention	DCH-27	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5		DCH-18
OPS-11.01B.4	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	The confidentiality and integrity of the logs is protected through appropriate security controls;	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
OPS-11.01B.4	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	The confidentiality and integrity of the logs is protected through appropriate security controls;	Functional	Intersects With	Sensitive Event Log & Security-Relevant Telemetry Data	MON-30	Mechanisms exist to protect sensitive and/or regulated data contained in event logs and security-relevant telemetry.	3		MON-03.1
OPS-11.01B.5	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	As far as technically possible, anonymised cloud service derived data is used only in a way so that no conclusions can be drawn about the usage behaviour of individual users of the cloud service customer;	Functional	Intersects With	De-Identification (Anonymization)	DCH-36	Mechanisms exist to de-identify sensitive and/or regulated data through (1) Anonymization; (2) De-identification; (3) Pseudonymization; and/or (4) Redaction.	5		DCH-23
OPS-11.01B.6	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	Cloud service derived data that has been fully anonymised and cannot be traced back to individual cloud service customers may be further processed and retained, provided no contractual or legal restrictions exist, otherwise immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary; and	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	3		DCH-21
OPS-11.01B.6	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	Cloud service derived data that has been fully anonymised and cannot be traced back to individual cloud service customers may be further processed and retained, provided no contractual or legal restrictions exist, otherwise immediate deletion if the purposes of the collection are fulfilled and further storage is no longer necessary; and	Functional	Intersects With	De-Identification (Anonymization)	DCH-36	Mechanisms exist to de-identify sensitive and/or regulated data through (1) Anonymization; (2) De-identification; (3) Pseudonymization; and/or (4) Redaction.	3		DCH-23

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-11.01B.7	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	Provision to cloud service customers according to contractual agreements.	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-07.1	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	3		CLD-06.2
OPS-11.02B	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	The cloud service provider specifies in the contractual agreements with cloud service customers all purposes for which cloud service derived data are collected and used, except for those purposes that are inherent to the general operation of all cloud services.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-30	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	3		PRI-05
OPS-11.02B	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	The cloud service provider specifies in the contractual agreements with cloud service customers all purposes for which cloud service derived data are collected and used, except for those purposes that are inherent to the general operation of all cloud services.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
OPS-11.01AC	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	Personal data is automatically removed from the log data before the cloud service provider processes it, as far as technically possible. The removal is done in a way that allows the cloud service provider to continue to use the log data for the purpose for which it was collected.	Functional	Intersects With	De-Identification (Anonymization)	DCH-36	Mechanisms exist to de-identify sensitive and/or regulated data through (1) Anonymization; (2) De-identification; (3) Pseudonymization; and/or (4) Redaction.	5		DCH-23
OPS-11.01AC	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	Personal data is automatically removed from the log data before the cloud service provider processes it, as far as technically possible. The removal is done in a way that allows the cloud service provider to continue to use the log data for the purpose for which it was collected.	Functional	Intersects With	Sensitive Event Log & Security-Relevant Telemetry Data	MON-30	Mechanisms exist to protect sensitive and/or regulated data contained in event logs and security-relevant telemetry.	5		MON-03.1
OPS-11.02AC	Logging and Monitoring - Policies and Procedures for Handling Cloud Service Derived Data and Account Data	Cloud service derived data, particularly log data, is included in regulatory compliance assessments.	Functional	Intersects With	Conformity Monitoring	CPL-05	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	3		CPL-03
OPS-12.01B	Logging and Monitoring - Access, Retention and Deletion	The requirements for the logging and monitoring of events and for the secure handling of cloud service derived data and cloud service provider data (cf. OPS-10, OPS-11) are implemented by technically supported procedures with regard to the following restrictions:	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
OPS-12.01B.1	Logging and Monitoring - Access, Retention and Deletion	Access only for authorised users and systems;	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
OPS-12.01B.1	Logging and Monitoring - Access, Retention and Deletion	Access only for authorised users and systems;	Functional	Intersects With	Query Parameter Audits of Personal Data (PD)	MON-29.2	Mechanisms exist to provide and implement the capability for auditing the parameters of user query events for data sets containing Personal Data (PD).	3		MON-06.1
OPS-12.01B.2	Logging and Monitoring - Access, Retention and Deletion	Retention for the specified period; and	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5		MON-10
OPS-12.01B.3	Logging and Monitoring - Access, Retention and Deletion	Deletion when further retention is no longer necessary for the purpose of collection.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	3		DCH-21
OPS-12.01B.3	Logging and Monitoring - Access, Retention and Deletion	Deletion when further retention is no longer necessary for the purpose of collection.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	3		MON-10
OPS-13.01B	Logging and Monitoring - Security Information and Event Management	The cloud service provider integrates relevant log data (cloud service derived data and cloud service provider data) into a Security Information and Event Management (SIEM) system to establish a seamless connection between logging, monitoring, and security incident management.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	8		MON-02
OPS-13.02B	Logging and Monitoring - Security Information and Event Management	The SIEM system is deployed within the cloud environment or externally and includes the following capabilities:	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02
OPS-13.02B.1	Logging and Monitoring - Security Information and Event Management	Standardisation of log data;	Functional	Intersects With	Correlate Monitoring Information	MON-08	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	3		MON-02.1
OPS-13.02B.2	Logging and Monitoring - Security Information and Event Management	Automated analysis to identify and correlate potential security incidents;	Functional	Intersects With	Correlate Monitoring Information	MON-08	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5		MON-02.1
OPS-13.02B.3	Logging and Monitoring - Security Information and Event Management	Capabilities to detect unusual behaviour and potential threats;	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		MON-16
OPS-13.02B.4	Logging and Monitoring - Security Information and Event Management	Real-time alerting to inform the incident response team of critical events;	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5		MON-01.4
OPS-13.02B.5	Logging and Monitoring - Security Information and Event Management	Reporting to the incident response team in case new information relevant to an event becomes available; and	Functional	Intersects With	Situational Awareness For Incidents	IRO-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	3		IRO-09
OPS-13.02B.5	Logging and Monitoring - Security Information and Event Management	Reporting to the incident response team in case new information relevant to an event becomes available; and	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	3		MON-01.4
OPS-13.02B.6	Logging and Monitoring - Security Information and Event Management	Automated response mechanisms for addressing security incidents.	Functional	Intersects With	Security Orchestration, Automation, and Response (SOAR)	OPS-08	Mechanisms exist to utilize Security Orchestration, Automation and Response (SOAR) tools to define, prioritize and automate the response to security incidents.	5		OPS-06
OPS-13.01AC	Logging and Monitoring - Security Information and Event Management	The cloud service provider validates the correct operation of event detection processes on appropriate assets. The appropriateness of the assets is identified in accordance with the asset classification schema (cf. AM-09).	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	3		IAO-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-13.01AC	Logging and Monitoring - Security Information and Event Management	The cloud service provider validates the correct operation of event detection processes on appropriate assets. The appropriateness of the assets is identified in accordance with the asset classification schema (cf. AM-09).	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	3		MON-01.8
OPS-13.02AC	Logging and Monitoring - Security Information and Event Management	Timely and appropriate remediation measures address any deviations identified during validation.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
OPS-13.03AC	Logging and Monitoring - Security Information and Event Management	If an event that can lead to security incidents is identified, incident handling activities by the cloud service provider are triggered without undue delay.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5		IRO-02
OPS-14.01B	Logging and Monitoring - Retention of the Logging Data	The cloud service provider retains the generated log data, including SIEM log data, and keeps it in an appropriate, unchangeable and aggregated form, regardless of the source of such data, so that a central, authorised evaluation of the data is possible.	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
OPS-14.01B	Logging and Monitoring - Retention of the Logging Data	The cloud service provider retains the generated log data, including SIEM log data, and keeps it in an appropriate, unchangeable and aggregated form, regardless of the source of such data, so that a central, authorised evaluation of the data is possible.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5		MON-10
OPS-14.02B	Logging and Monitoring - Retention of the Logging Data	Log data is deleted if it is no longer required for the purpose for which it was collected.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	3		DCH-21
OPS-14.02B	Logging and Monitoring - Retention of the Logging Data	Log data is deleted if it is no longer required for the purpose for which it was collected.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	3		MON-10
OPS-14.03B	Logging and Monitoring - Retention of the Logging Data	Between logging servers and the assets to be logged, authentication measures are in place to protect the integrity and authenticity of the information transmitted and stored. The transfer uses state of the art encryption or a dedicated administration network (out-of-band management).	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
OPS-14.03B	Logging and Monitoring - Retention of the Logging Data	Between logging servers and the assets to be logged, authentication measures are in place to protect the integrity and authenticity of the information transmitted and stored. The transfer uses state of the art encryption or a dedicated administration network (out-of-band management).	Functional	Intersects With	Remote Access Cryptographic Protections	NET-26.5	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	3		NET-14.2
OPS-15.01B	Logging and Monitoring - Accountability	The log data generated - compromising both cloud service derived data and cloud service provider data - enables unambiguous identification of user access at the tenant level, supporting effective forensic analysis in the event of a security incident.	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-07.1	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	3		CLD-06.2
OPS-15.01B	Logging and Monitoring - Accountability	The log data generated - compromising both cloud service derived data and cloud service provider data - enables unambiguous identification of user access at the tenant level, supporting effective forensic analysis in the event of a security incident.	Functional	Intersects With	Audit Trails	MON-09.1	Mechanisms exist to link system access to individual users or service accounts.	8		MON-03.2
OPS-15.02B	Logging and Monitoring - Accountability	Each logged event includes a time/date stamp to ensure accurate and traceable records.	Functional	Intersects With	Time Stamps	MON-11	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs and security-relevant telemetry.	8		MON-07
OPS-15.03B	Logging and Monitoring - Accountability	The cloud service provider is able to support forensic analysis of incidents and to retain a chain of evidence. This implies that the cloud service provider capture the state of hardware objects and network communication during security events.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5		IRO-08
OPS-15.03B	Logging and Monitoring - Accountability	The cloud service provider is able to support forensic analysis of incidents and to retain a chain of evidence. This implies that the cloud service provider capture the state of hardware objects and network communication during security events.	Functional	Intersects With	Non-Repudiation	MON-34	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.	3		MON-09
OPS-15.01AC	Logging and Monitoring - Accountability	On request of the cloud service customer, the cloud service provider provides the logs relating to the cloud service customer in an appropriate form and in a timely manner so that the cloud service customer can investigate any incidents relating to them.	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-07.1	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	5		CLD-06.2
OPS-15.02AC	Logging and Monitoring - Accountability	The aforementioned logs are collected and maintained using controls and processes that preserve their integrity and reliability for security monitoring and incident investigation purposes. This implies, but is not limited to:	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	3		IRO-08
OPS-15.02AC	Logging and Monitoring - Accountability	The aforementioned logs are collected and maintained using controls and processes that preserve their integrity and reliability for security monitoring and incident investigation purposes. This implies, but is not limited to:	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
OPS-15.02AC.1	Logging and Monitoring - Accountability	Records are complete and have not been tampered with in any way;	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
OPS-15.02AC.2	Logging and Monitoring - Accountability	Logging systems are clock synchronised, logs include accurate timestamps;	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-11.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5		MON-07.1
OPS-15.02AC.3	Logging and Monitoring - Accountability	Copies of electronic evidence are provably identical to the originals; and	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5		IRO-08
OPS-15.02AC.4	Logging and Monitoring - Accountability	Any information system from which evidence has been gathered was operating correctly at the time the evidence was recorded.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	3		IRO-08
OPS-16.01B	Logging and Monitoring - Configuration	Access to system components for logging and monitoring in the cloud service provider's area of responsibility is restricted to authorised users and requires authentication with two or more factors.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
OPS-16.01B	Logging and Monitoring - Configuration	Access to system components for logging and monitoring in the cloud service provider's area of responsibility is restricted to authorised users and requires authentication with two or more factors.	Functional	Intersects With	Query Parameter Audits of Personal Data (PD)	MON-29.2	Mechanisms exist to provide and implement the capability for auditing the parameters of user query events for data sets containing Personal Data (PD).	5		MON-06.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-16.02B	Logging and Monitoring -	Changes to the configuration are made in accordance with the applicable policies (cf. DEV-03).	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	5		CHG-02
OPS-17.01B	Logging and Monitoring - Availability of the	The cloud service provider monitors the availability of the system components for logging and monitoring in its area of responsibility.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
OPS-17.01B	Logging and Monitoring - Availability of the	The cloud service provider monitors the availability of the system components for logging and monitoring in its area of responsibility.	Functional	Intersects With	Response To Event Log Processing Failures	MON-33	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	5		MON-05
OPS-17.02B	Logging and Monitoring - Availability of the Monitoring Software	Failures are automatically and timely reported to the cloud service provider's responsible departments so that these can assess the failures and take required action.	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	3		MON-01.4
OPS-17.02B	Logging and Monitoring - Availability of the	Failures are automatically and timely reported to the cloud service provider's responsible departments so that these can assess the failures and take required action.	Functional	Intersects With	Response To Event Log Processing Failures	MON-33	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	5		MON-05
OPS-17.01AC	Logging and Monitoring - Availability of the	The cloud service provider provides resilience for the logs and the associated infrastructure by defining, documenting and implementing measures to protect their integrity, availability and confidentiality.	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
OPS-17.01AC	Logging and Monitoring - Availability of the	The cloud service provider provides resilience for the logs and the associated infrastructure by defining, documenting and implementing measures to protect their integrity, availability and confidentiality.	Functional	Intersects With	Alternate Event Logging Capability	MON-35	Mechanisms exist to provide an alternate event logging capability in the event of a failure in primary audit capability.	3		MON-13
OPS-17.02AC	Logging and Monitoring - Availability of the	The system components for logging and monitoring are designed in such a way that the overall functionality is not restricted if individual components fail.	Functional	Intersects With	Alternate Event Logging Capability	MON-35	Mechanisms exist to provide an alternate event logging capability in the event of a failure in primary audit capability.	5		MON-13
OPS-18.01B	Managing Vulnerabilities - Policies and Procedures	Policies and procedures with technical and organisational measures are documented, communicated and provided in accordance with SP-01 to govern the timely identification and addressing of vulnerabilities in the system components used to provide the cloud service. These policies and procedures contain specifications regarding the following	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	8		VPM-01
OPS-18.01B.1	Managing Vulnerabilities - Policies and Procedures	Regular (proactive) identification of vulnerabilities through suitable measures, including vulnerability scans and penetration tests, considering typical vulnerability classes and Common Weaknesses (CWEs);	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
OPS-18.01B.1	Managing Vulnerabilities - Policies and Procedures	Regular (proactive) identification of vulnerabilities through suitable measures, including vulnerability scans and penetration tests, considering typical vulnerability classes and Common Weaknesses (CWEs);	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07
OPS-18.01B.2	Managing Vulnerabilities - Policies and Procedures	Assessing the severity of identified vulnerabilities using the Common Vulnerability Scoring System (CVSS);	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
OPS-18.01B.3	Managing Vulnerabilities - Policies and Procedures	Prioritising and implementing measures considering existing standards for timely remediation and/or mitigation of identified vulnerabilities based on severity according to defined time frames and with reference to commonly used scoring systems like the Exploit Prediction Scoring System (EPSS) and the Stakeholder-Specific Vulnerability Categorisation (SSVC);	Functional	Intersects With	Vulnerability Exploitation Analysis	VPM-04	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	5		VPM-03.1
OPS-18.01B.3	Managing Vulnerabilities - Policies and Procedures	Prioritising and implementing measures considering existing standards for timely remediation and/or mitigation of identified vulnerabilities based on severity according to defined time frames and with reference to commonly used scoring systems like the Exploit Prediction Scoring System (EPSS) and the Stakeholder-Specific Vulnerability Categorisation (SSVC);	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
OPS-18.01B.4	Managing Vulnerabilities - Policies and Procedures	Deployment of Security Patches;	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
OPS-18.01B.5	Managing Vulnerabilities - Policies and Procedures	Handling system components for which no measures for timely remediation or mitigation of vulnerabilities are initiated based on a risk assessment;	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2
OPS-18.01B.5	Managing Vulnerabilities - Policies and Procedures	Handling system components for which no measures for timely remediation or mitigation of vulnerabilities are initiated based on a risk assessment;	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	3		VPM-02
OPS-18.01B.6	Managing Vulnerabilities - Policies and Procedures	Interfaces to incident management in case vulnerabilites become incidents;	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	3		IRO-02
OPS-18.01B.7	Managing Vulnerabilities - Policies and Procedures	If AI-based tools are used for performing vulnerability scans or penetration tests, requirements for the comprehensible (traceable, transparent) documentation on the use of such tools and that these tools shall be used to support the cloud service provider's subject matter experts, not to replace them; and	Functional	Intersects With	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-02	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented	3		AAT-01
OPS-18.01B.8	Managing Vulnerabilities - Policies and Procedures	Providing information on the configuration of system components and cloud services, the existing vulnerabilities, and the available patches and/or mitigation measures, using widely adopted, preferably automated, formats.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	3		TDA-04.2
OPS-18.01B.8	Managing Vulnerabilities - Policies and Procedures	Providing information on the configuration of system components and cloud services, the existing vulnerabilities, and the available patches and/or mitigation measures, using widely adopted, preferably automated, formats.	Functional	Intersects With	Correlate Scanning Information	VPM-17	Automated mechanisms exist to correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.	3		VPM-06.9
OPS-18.02B	Managing Vulnerabilities - Policies and Procedures	The policies and procedures for the timely identification and addressing of vulnerabilities define that for vulnerabilities assessed to be 'critical', engagement has to begin in a timely manner after identification, even if this occurs outside regular working hours. They also define how such a vulnerability is engaged with.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
OPS-18.03B	Managing Vulnerabilities - Policies and Procedures	The policies and procedures for the timely identification and addressing of vulnerabilities also define that for vulnerabilities assessed to be 'high', engagement has to begin within one working day after their identification. They also define how such a vulnerability is engaged	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
OPS-18.04B	Managing Vulnerabilities - Policies and Procedures	The engagement with a vulnerability according to the policies and procedures for the timely identification and addressing of vulnerabilities includes regular follow-up of the vulnerability until its remediation.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
OPS-18.05B	Managing Vulnerabilities - Policies and Procedures	Based on a risk assessment (cf. OIS-07), the cloud service provider can decide not to remediate or mitigate identified vulnerabilities. Such a risk assessment and the compensating or mitigating measures are reviewed regularly and in case of significant changes to the cloud service.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
OPS-18.05B	Managing Vulnerabilities - Policies and Procedures	Based on a risk assessment (cf. OIS-07), the cloud service provider can decide not to remediate or mitigate identified vulnerabilities. Such a risk assessment and the compensating or mitigating measures are reviewed regularly and in case of significant changes to the cloud service.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		RSK-06.2
OPS-19.01B	Managing Incidents and Crashes - Policies and Procedures	Policies and procedures with technical and organisational measures are documented, communicated, and provided in accordance with SP-01 to govern the timely identification and management of incidents and crashes in the system components used to provide the cloud service or of parts or the whole cloud service. These policies and procedures include specifications regarding the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-19.01B	Managing Incidents and Crashes - Policies and Procedures	Policies and procedures with technical and organisational measures are documented, communicated, and provided in accordance with SP-01 to govern the timely identification and management of incidents and crashes in the system components used to provide the cloud service or of parts or the whole cloud service. These policies and procedures include specifications regarding the following aspects:	Functional	Intersects With	Incident Response Operations	IRO-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5		IRO-01
OPS-19.01B.1	Managing Incidents and Crashes - Policies and Procedures	Classification and prioritisation of incidents and crashes;	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5		IRO-02.4
OPS-19.01B.2	Managing Incidents and Crashes - Policies and Procedures	Standardised incident-handling procedures for addressing known issues;	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5		IRO-02
OPS-19.01B.3	Managing Incidents and Crashes - Policies and Procedures	Escalation rules and procedures, including criteria for triggering Security Incident Management (SIM) processes in accordance with SIM-02 or internal incident management procedures;	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	3		IRO-02.4
OPS-19.01B.3	Managing Incidents and Crashes - Policies and Procedures	Escalation rules and procedures, including criteria for triggering Security Incident Management (SIM) processes in accordance with SIM-02 or internal incident management procedures;	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	3		IRO-04
OPS-19.01B.4	Managing Incidents and Crashes - Policies and Procedures	Knowledge sources for incidents and crashes;	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
OPS-19.01B.5	Managing Incidents and Crashes - Policies and Procedures	Criteria for determining when crashes are classified as incidents and when they trigger incident management processes;	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	3		IRO-02.4
OPS-19.01B.6	Managing Incidents and Crashes - Policies and Procedures	Mechanisms ensuring that access to crash files is restricted to authorised personnel only;	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	3		IAC-08
OPS-19.01B.7	Managing Incidents and Crashes - Policies and Procedures	Safeguards to prevent exposure of sensitive, personal, or confidential data within crash files;	Functional	Intersects With	Sensitive Event Log & Security-Relevant Telemetry Data	MON-30	Mechanisms exist to protect sensitive and/or regulated data contained in event logs and security-relevant telemetry.	5		MON-03.1
OPS-19.01B.8	Managing Incidents and Crashes - Policies and Procedures	Encryption of crash files for storage and during transmission;	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	3		CRY-03
OPS-19.01B.8	Managing Incidents and Crashes - Policies and Procedures	Encryption of crash files for storage and during transmission;	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	3		CRY-05
OPS-19.01B.9	Managing Incidents and Crashes - Policies and Procedures	Access management, logging, and review processes for access logs of crash files; and	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	3		IAC-17
OPS-19.01B.9	Managing Incidents and Crashes - Policies and Procedures	Access management, logging, and review processes for access logs of crash files; and	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	3		MON-08
OPS-19.01B.10	Managing Incidents and Crashes - Policies and Procedures	Retention periods and secure deletion processes for crash files once no longer needed.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	3		DCH-21
OPS-19.01B.10	Managing Incidents and Crashes - Policies and Procedures	Retention periods and secure deletion processes for crash files once no longer needed.	Functional	Intersects With	Media & Data Retention	DCH-27	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	3		DCH-18
OPS-20.01B	Managing Incidents - Implementation	The cloud service provider identifies, records, classifies, prioritises, and addresses incidents according to the policies and procedures for the identification and management of incidents and crashes (cf. OPS-19).	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8		IRO-02
OPS-21.01B	Managing Crashes - Implementation	Crashes of system components, parts of or the whole cloud service under the responsibility of the cloud service provider are identified, recorded, and addressed according to the policies and procedures for the identification and management of incidents and crashes (cf. OPS-19).	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
OPS-21.01B	Managing Crashes - Implementation	Crashes of system components, parts of or the whole cloud service under the responsibility of the cloud service provider are identified, recorded, and addressed according to the policies and procedures for the identification and management of incidents and crashes (cf. OPS-19).	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	3		IRO-02
OPS-22.01B	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	The cloud service provider performs penetration tests by qualified internal personnel or external penetration testers at least once a year and in case of significant changes to the cloud service in accordance with the policies for managing vulnerabilities (cf. OPS-18).	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8		VPM-07
OPS-22.02B	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	Penetration tests are carried out in accordance with a documented framework for penetration tests that outlines the number and types of penetration tests to be performed and the requirements for the qualification and competence of the personnel to perform such tests. The number and types of penetration tests to be performed are determined based on a risk assessment (cf. OIS-07).	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
OPS-22.03B	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	Penetration tests target the system components relevant to the provision of the cloud service in the area of responsibility of the cloud service provider. System components to be targeted are identified in a risk assessment.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
OPS-22.03B	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	Penetration tests target the system components relevant to the provision of the cloud service in the area of responsibility of the cloud service provider. System components to be targeted are identified in a risk assessment.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
OPS-22.04B	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	Penetration tests are carried out in accordance with test plans that cover all relevant system components and specify which system components are to be tested.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07
OPS-22.05B	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	If penetration tests follow multi-year test plans, each relevant system component is subjected to at least one penetration test within a maximum period of three years.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07
OPS-22.06B	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	The cloud service provider assesses the severity of identified vulnerabilities in accordance with the Common Vulnerability Scoring System (CVSS), in the latest version valid at the time of the assessment.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
OPS-22.07B	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	Actions for remediation or mitigation are taken in accordance with the time frames as defined in the policies for managing vulnerabilities (cf. OPS-18).	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-22.08B	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	The vulnerabilities discovered through penetration testing are subject to a root cause analysis. The root cause analysis enables an assessment of the extent to which similar vulnerabilities may be present in the cloud service.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
OPS-22.08B	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	The vulnerabilities discovered through penetration testing are subject to a root cause analysis. The root cause analysis enables an assessment of the extent to which similar vulnerabilities may be present in the cloud service.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	3		VPM-02
OPS-22.01AS	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	OPS-22.01AS, sharpening OPS-22.01B The cloud service provider performs penetration tests at least every six months and in case of significant changes to the cloud service by independent external penetration testers in accordance with the policies for managing vulnerabilities (cf. OPS-18). The external penetration testers are engaged only if the personnel supposed to perform the test verifiably meets the cloud service provider's qualification and competence requirements. Internal personnel for penetration tests may support the external personnel.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-19	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	8		VPM-07.1
OPS-22.02AS	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	OPS-22.02AS, sharpening OPS-22.02B Pre-launch and post-launch penetration tests are performed in accordance with a documented framework for penetration tests that outlines the number and types of penetration tests to be performed and the requirements for the qualification and competence of the personnel to perform such tests. The number and types of penetration tests to be performed are determined based on a risk assessment (cf. OIS-07).	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
OPS-22.03AS	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	OPS-22.03AS, sharpening OPS-22.03B Penetration tests target system components relevant to the provision of the cloud service in the area of responsibility of the cloud service provider. System components to be targeted are identified in a risk assessment incorporating, where applicable, threat modelling.	Functional	Intersects With	Threat Modeling	TDA-05.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	3		TDA-06.2
OPS-22.03AS	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	OPS-22.03AS, sharpening OPS-22.03B Penetration tests target system components relevant to the provision of the cloud service in the area of responsibility of the cloud service provider. System components to be targeted are identified in a risk assessment incorporating, where applicable, threat modelling.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
OPS-22.01AC	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	Penetration tests are performed based on reviews of the architecture and configuration of the system components, and of the cloud service provider's source code.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-04	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	3		SEA-02
OPS-22.01AC	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	Penetration tests are performed based on reviews of the architecture and configuration of the system components, and of the cloud service provider's source code.	Functional	Intersects With	Static Code Analysis	TDA-17.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	3		TDA-09.2
OPS-22.02AC	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	The cloud service provider designs a multi-year test plan for its penetration testing activities.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07
OPS-22.03AC	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	The cloud service provider reviews the effectiveness of penetration tests on system components at least annually, and in case of significant changes to the cloud service.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07
OPS-22.04AC	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	The cloud service provider uses the threat modelling process to prioritise system components with the highest risk exposure for penetration testing by systematically analysing cloud components, services, data flows, trust boundaries and assets critical to the cloud service to enumerate potential threats, vulnerabilities, and attack	Functional	Intersects With	Threat Modeling	TDA-05.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5		TDA-06.2
OPS-22.05AC	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	The cloud service provider correlates the possible exploits of discovered vulnerabilities with previous information security incidents to identify if the vulnerability may have been exploited before its discovery.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
OPS-22.05AC	Managing Vulnerabilities, Incidents and Crashes - Penetration Tests	The cloud service provider correlates the possible exploits of discovered vulnerabilities with previous information security incidents to identify if the vulnerability may have been exploited before its discovery.	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-17	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	3		MON-11.3
OPS-23.01B	Managing Vulnerabilities, Incidents and Crashes - Measurements, Analyses and Assessments of Procedures	The cloud service provider regularly measures, analyses and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness.	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	3		GOV-05
OPS-23.01B	Managing Vulnerabilities, Incidents and Crashes - Measurements, Analyses and Assessments of Procedures	The cloud service provider regularly measures, analyses and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
OPS-23.01B	Managing Vulnerabilities, Incidents and Crashes - Measurements, Analyses and Assessments of Procedures	The cloud service provider regularly measures, analyses and assesses the procedures with which vulnerabilities and incidents are handled to verify their continued suitability, appropriateness and effectiveness.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	3		VPM-01
OPS-23.02B	Managing Vulnerabilities, Incidents and Crashes - Measurements, Analyses and Assessments of Procedures	Results are evaluated at least quarterly in a documented form by responsible individuals or groups of the cloud service provider to initiate continuous improvement actions and to verify their effectiveness.	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5		GOV-05
OPS-24.01B	Involvement of Cloud Service Customers in the Event of Incidents	The cloud service provider periodically informs the cloud service customer on the status of incidents affecting the cloud service customer, or, where appropriate and necessary, involve the customer in the resolution, in a manner consistent with the contractual agreements.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
OPS-24.01B	Involvement of Cloud Service Customers in the Event of Incidents	The cloud service provider periodically informs the cloud service customer on the status of incidents affecting the cloud service customer, or, where appropriate and necessary, involve the customer in the resolution, in a manner consistent with the contractual	Functional	Intersects With	Situational Awareness For Incidents	IRO-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	3		IRO-09
OPS-24.02B	Involvement of Cloud Service Customers in the Event of Incidents	As soon as an incident has been resolved from the cloud service provider's perspective, the cloud service customer is informed about the actions taken according to the contractual agreements.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
OPS-24.01AC	Involvement of Cloud Service Customers in the Event of Incidents	The cloud service provider defines and documents procedures in contractual agreements with cloud service customers that specify the involvement of the customer in confirming, within a specified time period, that a resolution has effectively addressed the root cause of an incident.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	3		IRO-10
OPS-25.01B	Managing Vulnerabilities, Incidents and Crashes - Vulnerability Scans	System components in the area of responsibility of the cloud service provider for the provision of the cloud service are subject to vulnerability scans at least once a month in accordance with the policies for handling vulnerabilities (cf. OPS-18). These vulnerability scans include a comparison of software component data against up-to-date vulnerability databases (e.g., CVE, EUVD, etc.) to identify known	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8		VPM-06

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-25.02B	Managing Vulnerabilities, Incidents and Crashes - Vulnerability Scans	The cloud service provider assesses the severity of vulnerabilities in accordance with defined criteria.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
OPS-25.03B	Managing Vulnerabilities, Incidents and Crashes - Vulnerability Scans	Measures for timely remediation or mitigation are initiated within defined time frame.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
OPS-25.04B	Managing Vulnerabilities, Incidents and Crashes - Vulnerability Scans	The results of the vulnerability scans are used to update the cloud service provider's SIEM system (cf. OPS-13) rules, enabling the system to detect when known vulnerabilities are being actively exploited.	Functional	Intersects With	Correlate Monitoring Information	MON-08	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	3		MON-02.1
OPS-25.04B	Managing Vulnerabilities, Incidents and Crashes - Vulnerability Scans	The results of the vulnerability scans are used to update the cloud service provider's SIEM system (cf. OPS-13) rules, enabling the system to detect when known vulnerabilities are being actively exploited.	Functional	Intersects With	Correlate Scanning Information	VPM-17	Automated mechanisms exist to correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.	5		VPM-06.9
OPS-25.01AS	Managing Vulnerabilities, Incidents and Crashes - Vulnerability Scans	OPS-25.01AS, sharpening OPS-25.01B System components in the area of responsibility of the cloud service provider for the provision of the cloud service are subject to vulnerability scans at least once a day in accordance with the policies for handling vulnerabilities (cf. OPS-18). These vulnerability scans include a comparison of software component data against up-to-date vulnerability databases (e.g., CVE, EUVD, etc.) to identify known	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8		VPM-06
OPS-25.02AS	Managing Vulnerabilities, Incidents and Crashes - Vulnerability Scans	OPS-25.02AS, sharpening OPS-25.02B The cloud service provider assesses the severity of vulnerabilities using the latest version of the Common Vulnerability Scoring System (CVSS) valid at the time of the assessment.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
OPS-25.01AC	Managing Vulnerabilities, Incidents and Crashes - Vulnerability Scans	Time frames for the initiation of remediation or mitigation efforts after a vulnerability is identified are defined and monitored according to a risk-based classification framework. This framework incorporates, but is not limited to, the CVSS severity level of vulnerabilities.	Functional	Intersects With	Vulnerability Exploitation Analysis	VPM-04	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	3		VPM-03.1
OPS-25.01AC	Managing Vulnerabilities, Incidents and Crashes - Vulnerability Scans	Time frames for the initiation of remediation or mitigation efforts after a vulnerability is identified are defined and monitored according to a risk-based classification framework. This framework incorporates, but is not limited to, the CVSS severity level of vulnerabilities.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
OPS-26.01B	Managing Vulnerabilities, Incidents and Crashes - System Hardening	System components in the production environment used to provide the cloud service under the cloud service provider's responsibility are hardened according to generally accepted industry standards.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	8		CFG-02
OPS-26.02B	Managing Vulnerabilities, Incidents and Crashes - System Hardening	The hardening requirements for each system component are documented.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02
OPS-26.03B	Managing Vulnerabilities, Incidents and Crashes - System Hardening	If non-modifiable ('immutable') images are used, compliance with the hardening specifications, as defined in the hardening requirements, is checked upon creation of the images.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
OPS-26.03B	Managing Vulnerabilities, Incidents and Crashes - System Hardening	If non-modifiable ('immutable') images are used, compliance with the hardening specifications, as defined in the hardening requirements, is checked upon creation of the images.	Functional	Intersects With	Virtual Machine Images	SEA-23.1	Mechanisms exist to ensure the integrity of virtual machine images at all times.	3		CLD-05
OPS-26.04B	Managing Vulnerabilities, Incidents and Crashes - System Hardening	Configurations and log files (cloud service provider data) regarding the continuous availability of the aforementioned immutable images are retained.	Functional	Intersects With	Retention Of Previous Configurations	CFG-09	Mechanisms exist to retain previous versions of secure baseline configuration to support roll back.	3		CFG-02.3
OPS-26.04B	Managing Vulnerabilities, Incidents and Crashes - System Hardening	Configurations and log files (cloud service provider data) regarding the continuous availability of the aforementioned immutable images are retained.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	3		MON-10
OPS-26.05B	Managing Vulnerabilities, Incidents and Crashes - System Hardening	The cloud service provider implements monitoring measures to ensure system components comply with hardening specifications.	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	5		CFG-06
OPS-26.06B	Managing Vulnerabilities, Incidents and Crashes - System Hardening	Identified deviations from these specifications are timely reported to the appropriate departments for immediate assessment and action.	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	3		CFG-06
OPS-26.06B	Managing Vulnerabilities, Incidents and Crashes - System Hardening	Identified deviations from these specifications are timely reported to the appropriate departments for immediate assessment and action.	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	3		MON-01.4
OPS-26.05AS	Managing Vulnerabilities, Incidents and Crashes - System Hardening	OPS-26.05AS, sharpening OPS-26.05B System components in the cloud service provider's area of responsibility are automatically monitored for compliance with hardening specifications.	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	8		CFG-06
OPS-27.01B	Managing Vulnerabilities - Patch Management Policies and Procedures	Policies and procedures with technical and organisational measures are documented, communicated and provided in accordance with SP-01 to ensure system components under the responsibility of the cloud service provider are patched within a suitable time frame depending on contractual agreements and identified vulnerabilities or exploits. These policies and procedures contain specifications regarding the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
OPS-27.01B	Managing Vulnerabilities - Patch Management Policies and Procedures	Policies and procedures with technical and organisational measures are documented, communicated and provided in accordance with SP-01 to ensure system components under the responsibility of the cloud service provider are patched within a suitable time frame depending on contractual agreements and identified vulnerabilities or exploits. These policies and procedures contain specifications regarding the following aspects:	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8		VPM-05
OPS-27.01B.1	Managing Vulnerabilities - Patch Management Policies and Procedures	Software is kept up-to-date, including timely deployment of security patches;	Functional	Intersects With	Stable Versions	AST-37.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	3		VPM-04.1
OPS-27.01B.1	Managing Vulnerabilities - Patch Management Policies and Procedures	Software is kept up-to-date, including timely deployment of security patches;	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
OPS-27.01B.2	Managing Vulnerabilities - Patch Management Policies and Procedures	Patches are scheduled within maintenance windows, where applicable, to minimise service disruption; and	Functional	Intersects With	Timely Maintenance	MNT-04	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	3		MNT-03
OPS-27.01B.2	Managing Vulnerabilities - Patch Management Policies and Procedures	Patches are scheduled within maintenance windows, where applicable, to minimise service disruption; and	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	3		VPM-05
OPS-27.01B.3	Managing Vulnerabilities - Patch Management Policies and Procedures	Patches are tested in non-production environments before they are rolled out into the production environment, provided testing was successful. Mechanisms are in place to revert to previous software versions in case of unexpected issues.	Functional	Intersects With	Retention Of Previous Configurations	CFG-09	Mechanisms exist to retain previous versions of secure baseline configuration to support roll back.	3		CFG-02.3

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-27.01B.3	Managing Vulnerabilities - Patch Management Policies and Procedures	Patches are tested in non-production environments before they are rolled out into the production environment, provided testing was successful. Mechanisms are in place to revert to previous software versions in case of unexpected issues.	Functional	Intersects With	Test, Validate & Document Changes	CHG-07	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented into production.	3		CHG-02.2
OPS-27.02B	Managing Vulnerabilities - Patch Management Policies and Procedures	Patch management procedures are harmonised with the cloud service provider's overall software change management process (cf. DEV-03).	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	5		CHG-01
OPS-27.02B	Managing Vulnerabilities - Patch Management Policies and Procedures	Patch management procedures are harmonised with the cloud service provider's overall software change management process (cf. DEV-03).	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	3		VPM-05
OPS-27.03B	Managing Vulnerabilities - Patch Management Policies and Procedures	According to the measures and procedures of the overall change management, patches provided by third parties are identified, tested and deployed.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
OPS-27.04B	Managing Vulnerabilities - Patch Management Policies and Procedures	Systems are scanned after application of patches to ensure vulnerabilities and exploits are remediated and no known or unmitigated vulnerabilities or exploits were deployed.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
OPS-27.03AS	Managing Vulnerabilities - Patch Management Policies and Procedures	OPS-27.03AS, sharpening OPS-27.03B According to the measures and procedures of the overall change management, patches provided by third parties are identified, tested and deployed in an automated manner. In case of patches where manual intervention is required, an exception handling process for manual patching is defined.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
OPS-28.01B	Managing Vulnerabilities - Patch Management Implementation	The cloud service provider designs, implements and maintains technical and organisational measures for the deployment of patches on the systems and applications under its responsibility according to the patch management policies and procedures (cf. OPS-27).	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	8		VPM-05
OPS-29.01B	Managing Vulnerabilities, Incidents and Crashes - Externally Sourced Components	The cloud service provider designs, implements and maintains technical and organisational measures to manage updates to system components used to provide the cloud service that incorporate third-party or open-source libraries. This includes:	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5		TDA-04.2
OPS-29.01B	Managing Vulnerabilities, Incidents and Crashes - Externally Sourced Components	The cloud service provider designs, implements and maintains technical and organisational measures to manage updates to system components used to provide the cloud service that incorporate third-party or open-source libraries. This includes:	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
OPS-29.01B.1	Managing Vulnerabilities, Incidents and Crashes - Externally Sourced Components	Regularly identifying available updates and known vulnerabilities in third-party or open-source libraries used within applications;	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	3		TDA-04.2
OPS-29.01B.1	Managing Vulnerabilities, Incidents and Crashes - Externally Sourced Components	Regularly identifying available updates and known vulnerabilities in third-party or open-source libraries used within applications;	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
OPS-29.01B.2	Managing Vulnerabilities, Incidents and Crashes - Externally Sourced Components	Evaluating the potential impact of identified updates and vulnerabilities on the applications and the overall security posture;	Functional	Intersects With	Vulnerability Exploitation Analysis	VPM-04	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	5		VPM-03.1
OPS-29.01B.3	Managing Vulnerabilities, Incidents and Crashes - Externally Sourced Components	Implementing necessary updates and patches in a timely manner to address identified vulnerabilities; and	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
OPS-29.01B.4	Managing Vulnerabilities, Incidents and Crashes - Externally Sourced Components	Continuously monitoring applications to ensure updates are effectively applied and no known or unmitigated vulnerabilities are introduced.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-06.2	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5		VPM-04
OPS-30.01B	Separation of Datasets - Policies and Procedures	Based on a risk assessment (cf. OIS-07), the cloud service provider established policies and procedures with technical and organisational measures to ensure separation of cloud service customer data between different customers and between customers and the cloud service provider. These policies and procedures are documented, communicated and provided in accordance with SP-01 and contain specifications regarding the client separation based on a documented cloud layer model and include the following:	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	8		CLD-06
OPS-30.01B	Separation of Datasets - Policies and Procedures	Based on a risk assessment (cf. OIS-07), the cloud service provider established policies and procedures with technical and organisational measures to ensure separation of cloud service customer data between different customers and between customers and the cloud service provider. These policies and procedures are documented, communicated and provided in accordance with SP-01 and contain specifications regarding the client separation based on a documented cloud layer model and include the following:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
OPS-30.01B.1	Separation of Datasets - Policies and Procedures	Illustration of which cloud layers are used for the particular cloud service. The used cloud layers should be appropriate to enable client separation;	Functional	Intersects With	Cloud Security Architecture	CLD-05	Mechanisms exist to ensure that the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud deployments.	3		CLD-02
OPS-30.01B.1	Separation of Datasets - Policies and Procedures	Illustration of which cloud layers are used for the particular cloud service. The used cloud layers should be appropriate to enable client separation;	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	3		CLD-06
OPS-30.01B.2	Separation of Datasets - Policies and Procedures	Measures used to separate cloud service customer data along the used cloud layers. Those measures are categorised according to the protection goals of confidentiality, integrity and availability and if they are preventive, detective or reactive measures;	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5		CLD-06
OPS-30.01B.2	Separation of Datasets - Policies and Procedures	Measures used to separate cloud service customer data along the used cloud layers. Those measures are categorised according to the protection goals of confidentiality, integrity and availability and if they are preventive, detective or reactive measures;	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	3		NET-06
OPS-30.01B.3	Separation of Datasets - Policies and Procedures	Monitoring and compliance with these measures; and	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	3		CFG-06
OPS-30.01B.3	Separation of Datasets - Policies and Procedures	Monitoring and compliance with these measures; and	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
OPS-30.01B.4	Separation of Datasets - Policies and Procedures	Initiation of suitable measures in the event of deviations.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	3		IRO-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-31.01B	Separation of Datasets - Implementation	The cloud service provider designs, implements and maintains measures and procedures against threats to the separation of data sets according to the policies and procedures of OPS-30. The measures address prevention against, detection of and reaction to any incidents infringing the separation.	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	8		CLD-06
OPS-31.02B	Separation of Datasets - Implementation	Cloud service customer data stored and processed on shared virtual and physical resources is securely and strictly separated according to a documented approach based on OIS-07 risk assessment and following policies on cryptography (cf. CRY-01) to ensure the confidentiality and integrity of this data.	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5		CLD-06
OPS-31.02B	Separation of Datasets - Implementation	Cloud service customer data stored and processed on shared virtual and physical resources is securely and strictly separated according to a documented approach based on OIS-07 risk assessment and following policies on cryptography (cf. CRY-01) to ensure the confidentiality and integrity of this data.	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	3		CRY-05
OPS-31.03B	Separation of Datasets - Implementation	The risk assessment is reviewed as needed, especially in case of changes to the architecture of the cloud service, and at least annually. Measures are adjusted or improved as appropriate to ensure they remain commensurate with the risks.	Functional	Intersects With	Risk Assessment Update	RSK-13.2	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	5		RSK-07
OPS-32.01B	Confidential Computing - Policies and Procedures	If the cloud service comprises capabilities for confidential computing, policies and procedures and technical safeguards are documented, communicated and provided according to SP-01, in which the following aspects are described:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
OPS-32.01B	Confidential Computing - Policies and Procedures	If the cloud service comprises capabilities for confidential computing, policies and procedures and technical safeguards are documented, communicated and provided according to SP-01, in which the following aspects are described:	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.01B.1	Confidential Computing - Policies and Procedures	Purpose and scope, including which information security risks on the cloud service provider's side are to be mitigated through the use of confidential computing (cf. OIS-07) and how the cloud service customers can use the provided features to manage information security risks on their side;	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
OPS-32.01B.1	Confidential Computing - Policies and Procedures	Purpose and scope, including which information security risks on the cloud service provider's side are to be mitigated through the use of confidential computing (cf. OIS-07) and how the cloud service customers can use the provided features to manage information security risks on their side;	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.01B.2	Confidential Computing - Policies and Procedures	Available confidential computing technologies;	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.01B.3	Confidential Computing - Policies and Procedures	Determination of which parts of the cloud stack are protected with each technology and where third-party access is possible;	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-09	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	3		IAO-03
OPS-32.01B.3	Confidential Computing - Policies and Procedures	Determination of which parts of the cloud stack are protected with each technology and where third-party access is possible;	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.01B.4	Confidential Computing - Policies and Procedures	Listing of involved suppliers/service organisations; and	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
OPS-32.01B.5	Confidential Computing - Policies and Procedures	Utilisation of Trusted Execution Environments (TEEs) or secure enclaves.	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.02B	Confidential Computing - Policies and Procedures	The cloud service provider provides its customers with information on the aspects specified in OPS-32.01B according to PSS-01.	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04
OPS-32.03B	Confidential Computing - Policies and Procedures	Additional aspects addressed by the policies and procedures for confidential computing, not necessarily included in the information provided to the cloud service customers, include:	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.03B.1	Confidential Computing - Policies and Procedures	Responsibilities for the implementation and monitoring of confidential computing measures;	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	3		HRS-03
OPS-32.03B.2	Confidential Computing - Policies and Procedures	Security requirements to ensure the confidentiality, integrity, and authenticity of the data during processing; and	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.03B.3	Confidential Computing - Policies and Procedures	Relevant legal and regulatory requirements applicable to confidential computing.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
OPS-32.03B.4	Confidential Computing - Policies and Procedures	These security requirements to ensure the confidentiality, integrity, and authenticity of the data during processing include that:	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.03B.5	Confidential Computing - Policies and Procedures	Neither the cloud service provider nor any other unauthorised entity shall be able to access the cloud service customer data or the keys used for protecting that data; and	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
OPS-32.03B.5	Confidential Computing - Policies and Procedures	Neither the cloud service provider nor any other unauthorised entity shall be able to access the cloud service customer data or the keys used for protecting that data; and	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.03B.6	Confidential Computing - Policies and Procedures	Cryptographic algorithms that comply with the cloud service provider's policy for the use of cryptographic mechanisms (cf. CRY-01) are used.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic	5		CRY-01
OPS-32.01AC	Confidential Computing - Policies and Procedures	The cloud service provider documents and implements a technical framework for confidential computing, demonstrating how certain information security risks are mitigated (cf. OIS-07). The framework includes at least the following procedures and technical safeguards:	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.01AC.1	Confidential Computing - Policies and Procedures	Usage of Trusted Execution Environments (TEEs) or secure enclaves to process sensitive data (data in use) in a protected environment;	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.01AC.2	Confidential Computing - Policies and Procedures	Documentation of all associated interfaces;	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04
OPS-32.01AC.3	Confidential Computing - Policies and Procedures	Consideration of available hardware attestations;	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-32.01AC.4	Confidential Computing - Policies and Procedures	Utilisation of encryption techniques to secure data during processing, including secure key management;	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic	5		CRY-01
OPS-32.01AC.4	Confidential Computing - Policies and Procedures	Utilisation of encryption techniques to secure data during processing, including secure key management;	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
OPS-32.01AC.5	Confidential Computing - Policies and Procedures	Remote attestation to verify the identity and measured state of the TEE as well as code executed within the TEE;	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-32.01AC.6	Confidential Computing - Policies and Procedures	Implementation of monitoring and logging mechanisms to detect and respond to security incidents;	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
OPS-32.01AC.7	Confidential Computing - Policies and Procedures	Conducting security reviews and penetration tests (cf. OPS-22) regularly as well as on an event-driven basis to verify the effectiveness of confidential computing measures; and	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07
OPS-32.01AC.8	Confidential Computing - Policies and Procedures	Performing regular updates on the Trusted Computing Base of the TEE.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	3		VPM-05
OPS-33.01B	Confidential Computing - Remote Attestation	If the cloud service comprises capabilities for confidential computing, the cloud service provider offers remote attestation functionalities for data in-use protection.	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-33.02B	Confidential Computing - Remote Attestation	Remote attestation functionalities are based on cryptographic means rooted in trusted hard- and software.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic	3		CRY-01
OPS-33.02B	Confidential Computing - Remote Attestation	Remote attestation functionalities are based on cryptographic means rooted in trusted hard- and software.	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-33.03B	Confidential Computing - Remote Attestation	Remote attestation functionalities comprise an interface that allows the customer to verify the integrity of the remote attestation.	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
OPS-33.01AC	Confidential Computing - Remote Attestation	The cloud service provider clearly defines, documents and communicates the available attestation levels.	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04
OPS-33.02AC	Confidential Computing - Remote Attestation	The information is part of the guidelines and recommendations for the secure use of the cloud service provided (cf. PSS-01).	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04
OPS-34.01B	Container Management - Policies and Procedures	Policies and procedures with technical and organisational measures for the planning and management of containers are documented, communicated and provided in accordance with SP-01. These policies and procedures contain specifications for the entire container life cycle regarding at least the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
OPS-34.01B	Container Management - Policies and Procedures	Policies and procedures with technical and organisational measures for the planning and management of containers are documented, communicated and provided in accordance with SP-01. These policies and procedures contain specifications for the entire container life cycle regarding at least the following aspects:	Functional	Intersects With	Application Container	SEA-31	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	5		SEA-21
OPS-34.01B.1	Container Management - Policies and Procedures	Image creation, testing, and validation;	Functional	Intersects With	Virtual Machine Images	SEA-23.1	Mechanisms exist to ensure the integrity of virtual machine images at all times.	5		CLD-05
OPS-34.01B.2	Container Management - Policies and Procedures	Image storage and retrieval;	Functional	Intersects With	Virtual Machine Images	SEA-23.1	Mechanisms exist to ensure the integrity of virtual machine images at all times.	3		CLD-05
OPS-34.01B.3	Container Management - Policies and Procedures	Container deployment and management;	Functional	Intersects With	Application Container	SEA-31	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	5		SEA-21
OPS-34.01B.4	Container Management - Policies and Procedures	Container operations; and	Functional	Intersects With	Application Container	SEA-31	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	3		SEA-21
OPS-34.01B.5	Container Management - Policies and Procedures	Decommissioning of images and container.	Functional	Intersects With	Decommissioning	AST-36	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that: (1) Data is properly transitioned to new systems or archived; and (2) Hard drives are either destroyed or erased in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	3		AST-30
OPS-34.02B	Container Management - Policies and Procedures	The policies and procedures describe measures along the life cycle of containers and address at least the following aspects:	Functional	Intersects With	Application Container	SEA-31	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	3		SEA-21
OPS-34.02B.1	Container Management - Policies and Procedures	Containers are inventoried according to a documented process (cf. AM-02, AM-03, AM-09);	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02
OPS-34.02B.2	Container Management - Policies and Procedures	The need for malware protection is assessed and, if necessary, ensured (cf. OPS-05);	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04
OPS-34.02B.3	Container Management - Policies and Procedures	Logging and monitoring of events takes place along the container lifecycle and is executed according to a defined logging framework (cf. OPS-10, OPS-12);	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
OPS-34.02B.4	Container Management - Policies and Procedures	Cloud service customer data is separated based on a risk assessment (cf. OPS-30);	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5		CLD-06
OPS-34.02B.5	Container Management - Policies and Procedures	Access to the container host should take place in accordance with a roles and rights framework and a policy for managing access and access authorisations (cf. IAM-01, IAM-06);	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
OPS-34.02B.5	Container Management - Policies and Procedures	Access to the container host should take place in accordance with a roles and rights framework and a policy for managing access and access authorisations (cf. IAM-01, IAM-06);	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to	5		IAC-08
OPS-34.02B.5	Container Management - Policies and Procedures	Access to the container host should take place in accordance with a roles and rights framework and a policy for managing access and access authorisations (cf. IAM-01, IAM-06);	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	3		IAC-16

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
OPS-34.02B.6	Container Management - Policies and Procedures	Data stored on containers and data in transit should be encrypted as far as possible by the provider in accordance with the encryption policy (cf. CRY-01);	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	3		CRY-03
OPS-34.02B.6	Container Management - Policies and Procedures	Data stored on containers and data in transit should be encrypted as far as possible by the provider in accordance with the encryption policy (cf. CRY-01);	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	5		CRY-05
OPS-34.02B.7	Container Management - Policies and Procedures	Measures to ensure network security are established. This includes, for example, measures to detect network anomalies (cf. COS-01 and COS-03) such as unexpected data flows within the network or unwanted access attempts;	Functional	Intersects With	Network Intrusion Detection & Prevention Systems (NIDS & NIPS) Monitoring	MON-23	Mechanisms exist to monitor Network Intrusion Detection / Prevention Systems (NIDS / NIPS) technologies on critical systems, key network segments and network choke points.	3		MON-01.1
OPS-34.02B.7	Container Management - Policies and Procedures	Measures to ensure network security are established. This includes, for example, measures to detect network anomalies (cf. COS-01 and COS-03) such as unexpected data flows within the network or unwanted access attempts;	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	3		NET-06
OPS-34.02B.8	Container Management - Policies and Procedures	Changes to containers and images follow a regulated process (cf. DEV-03); and	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	5		CHG-02
OPS-34.02B.9	Container Management - Policies and Procedures	Hardening processes are carried out according to general industry standards to ensure that no unnecessary system services are executed (cf. PSS-11).	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02
OPS-34.01AC	Container Management - Policies and Procedures	The policies and procedures additionally describe measures along the life cycle of containers that address at least the following aspects:	Functional	Intersects With	Application Container	SEA-31	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	3		SEA-21
OPS-34.01AC.1	Container Management - Policies and Procedures	Container images are cryptographically signed and the signing key securely stored (cf. CRY-10) to ensure their authenticity and integrity;	Functional	Intersects With	Signed Components	CHG-13	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5		CHG-04.2
OPS-34.01AC.1	Container Management - Policies and Procedures	Container images are cryptographically signed and the signing key securely stored (cf. CRY-10) to ensure their authenticity and integrity;	Functional	Intersects With	Transmission of Cybersecurity & Data Protection Attributes	CRY-11	Mechanisms exist to associate Technology Assets, Applications and/or Services (TAAS) security attributes with information exchanged between	3		CRY-10
OPS-34.01AC.2	Container Management - Policies and Procedures	Container behaviour is monitored and restricted using runtime security controls; and	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
OPS-34.01AC.3	Container Management - Policies and Procedures	Software products used for the provision of container images are, where possible, regularly scanned for known vulnerabilities or malicious components in container images and dependencies.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
OPS-35.01B	Container Management - Implementation	The cloud service provider designs, implements and maintains technical and organisational measures for the planning and management of containers along their life cycle according to the container management policies and procedures (cf. OPS-34).	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
OPS-35.01B	Container Management - Implementation	The cloud service provider designs, implements and maintains technical and organisational measures for the planning and management of containers along their life cycle according to the container management policies and procedures (cf. OPS-34).	Functional	Intersects With	Application Container	SEA-31	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	5		SEA-21
5.7	Identity and Access Management (IAM)	Objective: Secure the authorisation and authentication of users of the cloud service provider to prevent unauthorised access.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	10		IAC-01
IAM-01.01B	Policy for Identities and Access Rights	The cloud service provider documents, communicates and makes available according to SP-01:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
IAM-01.01B	Policy for Identities and Access Rights	The cloud service provider documents, communicates and makes available according to SP-01:	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
IAM-01.01B.1	Policy for Identities and Access Rights	An authorisation framework based on role-based access control and the business and security requirements of the cloud service provider; and	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8		IAC-08
IAM-01.01B.2	Policy for Identities and Access Rights	A policy for managing identities and access rights for internal and external personnel of the cloud service provider and system components that have a role in automated authorisation processes of the cloud service provider.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
IAM-01.01B.2	Policy for Identities and Access Rights	A policy for managing identities and access rights for internal and external personnel of the cloud service provider and system components that have a role in automated authorisation processes of the cloud service provider.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
IAM-01.02B	Policy for Identities and Access Rights	For the purpose of the business and security requirements these documents address at least the following aspects:	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
IAM-01.02B.1	Policy for Identities and Access Rights	Aspects that are relevant for making access control decisions;	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	3		IAC-20
IAM-01.02B.2	Policy for Identities and Access Rights	Assignment of unique usernames;	Functional	Intersects With	Standardized Identifier Management (User Names)	IAC-13.1	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	8		IAC-09
IAM-01.02B.3	Policy for Identities and Access Rights	Granting and modifying identities and access rights based on the 'least-privilege-principle' and the 'need-to-know-principle';	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business	8		IAC-21
IAM-01.02B.4	Policy for Identities and Access Rights	Application of a role-based mechanism for assigning access rights;	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	8		IAC-08
IAM-01.02B.5	Policy for Identities and Access Rights	Definition of the supported identity and role-based access types, including an assignment of access control parameters and roles to be considered for each type;	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	3		IAC-08
IAM-01.02B.5	Policy for Identities and Access Rights	Definition of the supported identity and role-based access types, including an assignment of access control parameters and roles to be considered for each type;	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
IAM-01.02B.6	Policy for Identities and Access Rights	Segregation of duties between operational and monitoring functions ('Segregation of Duties');	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5		HRS-11
IAM-01.02B.7	Policy for Identities and Access Rights	Assigning and monitoring privileged access rights;	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5		IAC-16
IAM-01.02B.7	Policy for Identities and Access Rights	Assigning and monitoring privileged access rights;	Functional	Intersects With	Privileged Account Inventories	IAC-10.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	3		IAC-16.1
IAM-01.02B.8	Policy for Identities and Access Rights	Approval by authorised individual(s) or system(s) for granting or modifying identities and access rights before cloud service customer data, cloud service derived data and cloud service provider data can be accessed;	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
IAM-01.02B.9	Policy for Identities and Access Rights	Regular review of assigned identities and access rights;	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	5		IAC-17
IAM-01.02B.10	Policy for Identities and Access Rights	Blocking and removing identities or limiting access in the event of inactivity;	Functional	Intersects With	Disable Inactive Accounts	IAC-08.4	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5		IAC-15.3
IAM-01.02B.11	Policy for Identities and Access Rights	Specific measures for managing identities whose use is restricted to emergency recovery and similar scenarios;	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
IAM-01.02B.12	Policy for Identities and Access Rights	Time-based or event-driven removal or adjustment of access rights in the event of changes to job responsibility;	Functional	Intersects With	Change of Roles & Duties	IAC-04.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5		IAC-07.1
IAM-01.02B.13	Policy for Identities and Access Rights	Multi-factor authentication for users with privileged access;	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	3		IAC-16
IAM-01.02B.13	Policy for Identities and Access Rights	Multi-factor authentication for users with privileged access;	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
IAM-01.02B.13	Policy for Identities and Access Rights	Multi-factor authentication for users with privileged access;	Functional	Intersects With	Multi-Factor Authentication (MFA) For Network Access to Privileged Accounts	IAC-37.5	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5		IAC-06.1
IAM-01.02B.13	Policy for Identities and Access Rights	Multi-factor authentication for users with privileged access;	Functional	Intersects With	Multi-Factor Authentication (MFA) For Local Access to Privileged Accounts	IAC-37.7	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5		IAC-06.3
IAM-01.02B.14	Policy for Identities and Access Rights	Remote access and access across geographic boundaries;	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		NET-14
IAM-01.02B.15	Policy for Identities and Access Rights	Requirements for approving and documenting the management of identities and access rights; and	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
IAM-01.02B.16	Policy for Identities and Access Rights	Measures to be taken upon the detection of a potential identity compromise, such as disabling and removing the affected identities.	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	3		IAC-10
IAM-01.02B.16	Policy for Identities and Access Rights	Measures to be taken upon the detection of a potential identity compromise, such as disabling and removing the affected identities.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	3		IRO-02
IAM-01.03B	Policy for Identities and Access Rights	The cloud service provider is capable of producing a list of the currently granted cloud-based access rights for each identity under its responsibility.	Functional	Intersects With	User & Service Account Inventories	IAC-08.3	Mechanisms exist to maintain a current list of authorized users and service accounts.	5		IAC-01.3
IAM-01.03B	Policy for Identities and Access Rights	The cloud service provider is capable of producing a list of the currently granted cloud-based access rights for each identity under its responsibility.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	3		IAC-17
IAM-01.01AC	Policy for Identities and Access Rights	Access logs are reviewed at least every month in order to detect attempts of unauthorised access or suspicious access patterns.	Functional	Intersects With	Centralized Event Log & Security-Relevant Telemetry Review & Analysis	MON-05.1	Automated mechanisms exist to centrally collect, review and analyze event logs and security-relevant telemetry from multiple sources.	5		MON-02.2
IAM-01.01AC	Policy for Identities and Access Rights	Access logs are reviewed at least every month in order to detect attempts of unauthorised access or suspicious access patterns.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Analysis & Triage	MON-05.2	Mechanisms exist to ensure event log and security-relevant telemetry reviews include analysis and triage practices that integrate with the organization's established incident response processes.	3		MON-17
IAM-02.01B	Granting and Change of Identities and Access Rights	Specified procedures for granting and modifying identities and access rights for internal and external personnel of the cloud service provider as well as for system components involved in automated authorisation processes of the cloud service provider ensure compliance with the role and rights policies and procedures as well as the policy for managing identities and access rights.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	8		IAC-15
IAM-02.02B	Granting and Change of Identities and Access Rights	The aforementioned procedures include, but are not limited to:	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15
IAM-02.02B.1	Granting and Change of Identities and Access Rights	Processes and technical controls to restrict access to the cloud service provider's data and system functions to authorised personnel; and	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		IAC-20
IAM-02.02B.2	Granting and Change of Identities and Access Rights	Processes and technical controls to manage and verify access permissions within the cloud service provider's systems.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
IAM-02.02B.2	Granting and Change of Identities and Access Rights	Processes and technical controls to manage and verify access permissions within the cloud service provider's systems.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	5		IAC-17
IAM-02.03B	Granting and Change of Identities and Access Rights	If the cloud service provider defines break glass accounts for use in case of a non-availability of the main procedure for authentication, specific requirements and procedures for the secure usage of those accounts are defined and implemented.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
IAM-03.01B	Risk-Based Procedure for Locking and Withdrawal of Identities	The cloud service provider has a risk-based procedure in place for managing identities (cf. IAM-01), taking into account the types of data accessible via the identities of the internal and external personnel.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15
IAM-03.01B	Risk-Based Procedure for Locking and Withdrawal of Identities	The cloud service provider has a risk-based procedure in place for managing identities (cf. IAM-01), taking into account the types of data accessible via the identities of the internal and external personnel.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
IAM-03.02B	Risk-Based Procedure for Locking and Withdrawal of Identities	As part of this procedure, specific parameters for automatically locking and withdrawing access due to inactivity or indications of brute force attacks are defined, with exceptions for the identities whose use is restricted to emergency recovery and similar scenarios.	Functional	Intersects With	Account Lockout	CFG-04.1	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5		IAC-22
IAM-03.02B	Risk-Based Procedure for Locking and Withdrawal of Identities	As part of this procedure, specific parameters for automatically locking and withdrawing access due to inactivity or indications of brute force attacks are defined, with exceptions for the identities whose use is restricted to emergency recovery and similar scenarios.	Functional	Intersects With	Disable Inactive Accounts	IAC-08.4	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5		IAC-15.3

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
IAM-03.03B	Risk-Based Procedure for Locking and Withdrawal of Identities	The cloud service provider documents and implements a process for monitoring stolen and compromised credentials, which also includes disabling any identity for which an issue is identified. This process is implemented on all identities under the responsibility of the cloud service provider that have privileged access rights.	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5		IAC-10
IAM-03.03B	Risk-Based Procedure for Locking and Withdrawal of Identities	The cloud service provider documents and implements a process for monitoring stolen and compromised credentials, which also includes disabling any identity for which an issue is identified. This process is implemented on all identities under the responsibility of the cloud service provider that have privileged access rights.	Functional	Intersects With	Threat Intelligence Feeds	THR-04	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	3		THR-03
IAM-03.04B	Risk-Based Procedure for Locking and Withdrawal of Identities	The aforementioned process includes an exception mechanism to be applied if all identities needed to manage the situation are potentially compromised.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
IAM-03.03AS	Risk-Based Procedure for Locking and Withdrawal of Identities	IAM-03.03AS, sharpening IAM-03.03B The cloud service provider documents and implements a process for monitoring stolen and compromised credentials, which also includes disabling any identity for which an issue is identified. This process is implemented on all identities under the responsibility of the cloud service provider.	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5		IAC-10
IAM-03.01AC	Risk-Based Procedure for Locking and Withdrawal of Identities	The context of authentication attempts is monitored and suspicious events are, as relevant, flagged to authorised persons.	Functional	Intersects With	Adaptive Identification & Authentication	IAC-41	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.	5		IAC-13
IAM-03.01AC	Risk-Based Procedure for Locking and Withdrawal of Identities	The context of authentication attempts is monitored and suspicious events are, as relevant, flagged to authorised persons.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
IAM-03.02AC	Risk-Based Procedure for Locking and Withdrawal of Identities	The effectiveness of the procedures for locking and withdrawing identities is validated.	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	3		IAO-02
IAM-03.03AC	Risk-Based Procedure for Locking and Withdrawal of Identities	Timely and appropriate remediation measures address any deviations identified during validation.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
IAM-04.01B	Withdrawal or Adjustment of Access Rights as the Task Area Changes	Access rights are timely adjusted or revoked if the job responsibilities of the cloud service provider's internal or external personnel or the tasks of system components involved in the cloud service provider's automated authorisation processes change.	Functional	Intersects With	Change of Roles & Duties	IAC-04.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	8		IAC-07.1
IAM-04.02B	Withdrawal or Adjustment of Access Rights as the Task Area Changes	Privileged access rights are adjusted or revoked within 48 hours after the change taking effect.	Functional	Intersects With	Change of Roles & Duties	IAC-04.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5		IAC-07.1
IAM-04.03B	Withdrawal or Adjustment of Access Rights as the Task Area Changes	All other access rights are adjusted or revoked within 14 days.	Functional	Intersects With	Change of Roles & Duties	IAC-04.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5		IAC-07.1
IAM-04.04B	Withdrawal or Adjustment of Access Rights as the Task Area Changes	After revocation, the procedure for granting identities and access rights (cf. IAM-02) is repeated.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
IAM-04.05B	Withdrawal or Adjustment of Access Rights as the Task Area Changes	In cases of role changes where temporary access may need to be granted, these access rights are approved, time-limited and documented.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
IAM-04.05B	Withdrawal or Adjustment of Access Rights as the Task Area Changes	In cases of role changes where temporary access may need to be granted, these access rights are approved, time-limited and documented.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	3		IAC-16
IAM-05.01B	Regular Review of Access Rights	Identities and the associated access rights of internal and external personnel of the cloud service provider as well as of system components that play a role in automated authorisation processes of the cloud service provider are reviewed at least once a year and in case of significant changes to the cloud service to ensure that they still correspond to the actual area of use.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	8		IAC-17
IAM-05.02B	Regular Review of Access Rights	The review is carried out by authorised persons from the cloud service provider's organisational units, who can assess the appropriateness of the assigned access rights based on their knowledge of the task areas of the personnel or system components.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	5		IAC-17
IAM-05.03B	Regular Review of Access Rights	Identified deviations are dealt with timely, but no later than seven days after their detection, through appropriate modification or withdrawal of the access rights.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	5		IAC-17
IAM-05.04B	Regular Review of Access Rights	When revoking identities, the system ensures that all production associated system components (e.g., virtual machines, storage, access rights) are identified, reassigned, or deleted to prevent the creation of orphaned resources. Clear processes and technical controls are established to identify and handle any orphaned resources that occur despite preventive measures, ensuring their timely reassignment or secure deletion.	Functional	Intersects With	Decommissioning	AST-36	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are properly decommissioned so that: (1) Data is properly transitioned to new systems or archived; and (2) Hard drives are either destroyed or erased in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	3		AST-30
IAM-05.04B	Regular Review of Access Rights	When revoking identities, the system ensures that all production associated system components (e.g., virtual machines, storage, access rights) are identified, reassigned, or deleted to prevent the creation of orphaned resources. Clear processes and technical controls are established to identify and handle any orphaned resources that occur despite preventive measures, ensuring their timely reassignment or secure deletion.	Functional	Intersects With	Removal of Temporary / Emergency Accounts	IAC-11.1	Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.	5		IAC-15.2
IAM-05.05B	Regular Review of Access Rights	For system components that are not production associated, the cloud service provider designs, implements and maintains appropriate controls for the prevention of orphan resources based on a risk assessment (cf. OIS-07).	Functional	Intersects With	Removal of Temporary / Emergency Accounts	IAC-11.1	Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.	3		IAC-15.2

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
IAM-05.05B	Regular Review of Access Rights	For system components that are not production associated, the cloud service provider designs, implements and maintains appropriate controls for the prevention of orphan resources based on a risk assessment (cf. OIS-07).	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
IAM-05.01AC	Regular Review of Access Rights	Privileged access rights are reviewed at least every six months, and in case of significant changes to the cloud service.	Functional	Intersects With	Privileged Account Inventories	IAC-10.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	5		IAC-16.1
IAM-05.01AC	Regular Review of Access Rights	Privileged access rights are reviewed at least every six months, and in case of significant changes to the cloud service.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	5		IAC-17
IAM-06.01B	Privileged Access Rights	Privileged access rights for internal and external personnel as well as technical users of the cloud service provider are assigned and changed in accordance with the policy for managing identities and access rights (cf. IAM-01) or a separate specific policy.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8		IAC-16
IAM-06.02B	Privileged Access Rights	Privileged access rights are personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks ('need-to-know-principle').	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5		IAC-16
IAM-06.02B	Privileged Access Rights	Privileged access rights are personalised, limited in time according to a risk assessment and assigned as necessary for the execution of tasks ('need-to-know-principle').	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business	5		IAC-21
IAM-06.03B	Privileged Access Rights	Anonymous technical users are only accessed through authentication with a personalised identity.	Functional	Intersects With	Credential Sharing	IAC-23	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5		IAC-19
IAM-06.03B	Privileged Access Rights	Anonymous technical users are only accessed through authentication with a personalised identity.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-32	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	3		IAC-02
IAM-06.04B	Privileged Access Rights	Activities of users with privileged access rights are logged in order to detect any misuse of privileged access in suspicious cases.	Functional	Intersects With	Privileged Command Execution	IAC-10.4	Mechanisms exist to ensure privilege change requests require additional levels of authentication.	3		IAC-16.3
IAM-06.04B	Privileged Access Rights	Activities of users with privileged access rights are logged in order to detect any misuse of privileged access in suspicious cases.	Functional	Intersects With	Audit Trails	MON-09.1	Mechanisms exist to link system access to individual users or service accounts.	5		MON-03.2
IAM-06.05B	Privileged Access Rights	The logged information is automatically monitored for defined events that may indicate misuse.	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	3		MON-01.4
IAM-06.05B	Privileged Access Rights	The logged information is automatically monitored for defined events that may indicate misuse.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		MON-16
IAM-06.06B	Privileged Access Rights	When such an event is identified, the responsible personnel is automatically informed so that they can timely assess whether misuse has occurred and take corresponding action.	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5		MON-01.4
IAM-06.07B	Privileged Access Rights	In the event of proven misuse of privileged access rights, disciplinary measures are taken in accordance with HR-04.	Functional	Intersects With	Personnel Sanctions	HRS-10	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5		HRS-07
IAM-06.08B	Privileged Access Rights	For containers and images, activities of users with privileged access are logged according to OPS-10.	Functional	Intersects With	Audit Trails	MON-09.1	Mechanisms exist to link system access to individual users or service accounts.	3		MON-03.2
IAM-06.08B	Privileged Access Rights	For containers and images, activities of users with privileged access are logged according to OPS-10.	Functional	Intersects With	Application Container	SEA-31	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	3		SEA-21
IAM-06.09B	Privileged Access Rights	Access to the cloud service provider's administration interfaces requires the use of multi-factor authentication.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	8		IAC-06
IAM-06.09B	Privileged Access Rights	Access to the cloud service provider's administration interfaces requires the use of multi-factor authentication.	Functional	Intersects With	Multi-Factor Authentication (MFA) For Network Access to Privileged Accounts	IAC-37.5	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5		IAC-06.1
IAM-06.01AC	Privileged Access Rights	The cloud service provider maintains an inventory of the identities with privileged access rights under its responsibility. This inventory is kept up-to-date.	Functional	Intersects With	Privileged Account Inventories	IAC-10.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	8		IAC-16.1
IAM-06.02AC	Privileged Access Rights	The cloud service provider maintains a list of the personnel that is responsible for an identity assigned to a non-human entity within the cloud service provider's scope of responsibility. This list is reviewed every six months and in case of significant changes to the cloud service.	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment	AST-07.1	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	3		AST-03
IAM-06.02AC	Privileged Access Rights	The cloud service provider maintains a list of the personnel that is responsible for an identity assigned to a non-human entity within the cloud service provider's scope of responsibility. This list is reviewed every six months and in case of significant changes to the cloud service.	Functional	Intersects With	User & Service Account Inventories	IAC-08.3	Mechanisms exist to maintain a current list of authorized users and service accounts.	5		IAC-01.3
IAM-06.03AC	Privileged Access Rights	For privileged users, phishing-resistant multi-factor authentication such as FIDO2 security keys or comparable mechanisms using public key cryptography and domain binding are implemented.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
IAM-06.03AC	Privileged Access Rights	For privileged users, phishing-resistant multi-factor authentication such as FIDO2 security keys or comparable mechanisms using public key cryptography and domain binding are implemented.	Functional	Intersects With	Phishing-Resistant Multi-Factor Authentication (MFA)	IAC-37.2	Automated mechanisms exist to enforce phishing-resistant Multi-Factor Authentication (MFA) through authenticators that are cryptographically bound to the verifier's identity, preventing credential relay by an impersonating party.	8		
IAM-06.03AC	Privileged Access Rights	For privileged users, phishing-resistant multi-factor authentication such as FIDO2 security keys or comparable mechanisms using public key cryptography and domain binding are implemented.	Functional	Intersects With	Multi-Factor Authentication (MFA) For Network Access to Privileged Accounts	IAC-37.5	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5		IAC-06.1
IAM-06.04AC	Privileged Access Rights	Privileged access rights are enforced through a privileged access management (PAM) solution with support for 'just-in-time' elevation and 'just-enough' access.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8		IAC-16
IAM-07.01B	Access to Cloud Service Customer Data	The cloud service provider implements partitioning measures that are:	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5		CLD-06
IAM-07.01B	Access to Cloud Service Customer Data	The cloud service provider implements partitioning measures that are:	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
IAM-07.01B.1	Access to Cloud Service Customer Data	Sufficient for separating the system components for providing the cloud service from the system components of the cloud service provider's other information systems; and	Functional	Intersects With	Segregation From Enterprise Services	NET-08.2	Mechanisms exist to isolate sensitive and/or regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware and patch management) to those isolated network segments.	5		NET-06.4
IAM-07.01B.2	Access to Cloud Service Customer Data	Suitable for separating different cloud service customers from each other (cf. OPS-30 and OPS-31).	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5		CLD-06
IAM-07.02B	Access to Cloud Service Customer Data	The partitioning measures of the cloud service provider ensure that security incidents, if they compromise the system components storing the cloud service customer data, do not also compromise the system components that manage the access to them.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	3		NET-06
IAM-07.02B	Access to Cloud Service Customer Data	The partitioning measures of the cloud service provider ensure that security incidents, if they compromise the system components storing the cloud service customer data, do not also compromise the system components that manage the access to them.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-06	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	3		SEA-03
IAM-07.03B	Access to Cloud Service Customer Data	Unless prohibited by applicable law, the cloud service customer is informed by the cloud service provider whenever internal or external personnel of the cloud service provider reads or writes to the cloud service customer data processed, stored or transmitted in the cloud service or has accessed it without the prior consent of the cloud service customer. The information is provided whenever cloud service customer data is/was accessed in unencrypted form or the contractual agreements with customers do not explicitly exclude informing the customer of such access.	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	3		IAC-20
IAM-07.04B	Access to Cloud Service Customer Data	Unless contractually agreed otherwise, the information provided about the access contains the cause, time, duration, geographic location, type and scope of the access, as well as the retention time of other data generated during access, such as logs or copies containing cloud service customer data. The information is sufficiently detailed to enable subject matter experts of the cloud service customer to assess the risks of the access.	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	3		IAC-20
IAM-07.05B	Access to Cloud Service Customer Data	The information is provided in accordance with the contractual agreements, but no later than 72 hours from the initiation of the access.	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	3		IAC-20
IAM-07.06B	Access to Cloud Service Customer Data	The cloud service provider discloses, through contractual agreements and before offering its services, all instances where the cloud service provider may access cloud service customer data in unencrypted form while it is processed, stored or transmitted in the cloud service.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
IAM-07.03AS	Access to Cloud Service Customer Data	IAM-07.03AS, sharpening IAM-07.03B Access to cloud service customer data and cloud service derived data by internal or external personnel of the cloud service provider requires the prior consent of an authorised department of the cloud service customer, provided that the cloud service customer's data is accessible in unencrypted form or contractual agreements do not explicitly exclude such consent. Additionally, if encrypted data and its decryption key are stored separately within the same cloud environment, prior consent is required not only for accessing the decryption key but also for accessing the encrypted data itself	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	3		IAC-20
IAM-07.04AS	Access to Cloud Service Customer Data	IAM-07.04AS, sharpening IAM-07.04B Unless contractually agreed otherwise, the information provided for the consent contains the cause, time, duration, geographic location, type and scope of the access, as well as the retention time of other data generated during access, such as logs or copies containing cloud service customer data. The information is sufficiently detailed to enable subject matter experts of the cloud service customer to assess the risks of the access. In addition to the provided information, the cloud service provider specifies a time frame within which the cloud service customer shall respond to the access request.	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	3		IAC-20
IAM-07.06AS	Access to Cloud Service Customer Data	IAM-07.06AS, sharpening IAM-07.06B The cloud service provider discloses, through contractual agreements and before offering its services, all instances where the cloud service provider may access cloud service customer data or cloud service derived data in unencrypted form while it is processed, stored or transmitted in the cloud service.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
IAM-07.01AC	Access to Cloud Service Customer Data	If the cloud service provider might access the cloud service customer data transmitted, handled or stored in the cloud service in a non-encrypted way, the cloud service provider includes provisions through contractual agreements for cases in which seeking prior consent for such an access is not feasible.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
IAM-07.02AC	Access to Cloud Service Customer Data	In order to be able to directly or indirectly access cloud service customer data, any internal or external personnel of the cloud service provider has to pass an appropriate assessment, or has to instead be supervised by personnel who has passed an appropriate assessment (cf. HR-01). The cloud service provider verifies that one of these conditions is met before the access is granted. This applies to support operations as well.	Functional	Intersects With	Personnel Screening	HRS-05	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5		HRS-04
IAM-07.02AC	Access to Cloud Service Customer Data	In order to be able to directly or indirectly access cloud service customer data, any internal or external personnel of the cloud service provider has to pass an appropriate assessment, or has to instead be supervised by personnel who has passed an appropriate assessment (cf. HR-01). The cloud service provider verifies that one of these conditions is met before the access is granted. This applies to support operations as well.	Functional	Intersects With	Roles With Special Protection Measures	HRS-05.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	3		HRS-04.1
IAM-07.03AC	Access to Cloud Service Customer	If the performed access is supervised, the cloud service provider ensures that:	Functional	Intersects With	Privileged Command Execution	IAC-10.4	Mechanisms exist to ensure privilege change requests require additional levels of authentication.	3		IAC-16.3
IAM-07.03AC.1	Access to Cloud Service Customer Data	The mechanisms used to perform the supervised access allow the supervising personnel to authorise or deny individual actions of the supervisee and ask for explanations in real time;	Functional	Intersects With	Privileged Command Execution	IAC-10.4	Mechanisms exist to ensure privilege change requests require additional levels of authentication.	3		IAC-16.3
IAM-07.03AC.2	Access to Cloud Service Customer Data	Any access rights that are granted as part of the supervised access are revoked at the end of the operation;	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
IAM-07.03AC.3	Access to Cloud Service Customer	All operations that are performed as part of the supervised access are logged as administration actions;	Functional	Intersects With	Audit Trails	MON-09.1	Mechanisms exist to link system access to individual users or service accounts.	3		MON-03.2
IAM-07.03AC.4	Access to Cloud Service Customer Data	The supervisee and the device used to perform the supervised access are authenticated by the supervision solution;	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-32	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	3		IAC-02
IAM-07.03AC.4	Access to Cloud Service Customer Data	The supervisee and the device used to perform the supervised access are authenticated by the supervision solution;	Functional	Intersects With	Identification & Authentication for Devices	IAC-34	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	3		IAC-04
IAM-07.03AC.5	Access to Cloud Service Customer Data	The operations that the supervisee proposes and the actions of the supervising personnel are logged by the supervision solution, including operations that were denied; and	Functional	Intersects With	Audit Trails	MON-09.1	Mechanisms exist to link system access to individual users or service accounts.	3		MON-03.2
IAM-07.03AC.6	Access to Cloud Service Customer Data	Information flows towards the device of the supervisee are prevented by the supervision solution.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	3		NET-04

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
IAM-07.04AC	Access to Cloud Service Customer Data	If the cloud service customer is given access to interfaces for administrators and for end users as part of the cloud service, the cloud service provider separates these interfaces from one another and ensures that access paths for customer administrators differ from those for end users.	Functional	Intersects With	Privileged Account Separation	IAC-10.2	Mechanisms exist to separate privileged accounts between infrastructure environments to reduce the risk of a compromise in one infrastructure environment from laterally affecting other infrastructure environments.	5		IAC-16.2
IAM-07.04AC	Access to Cloud Service Customer Data	If the cloud service customer is given access to interfaces for administrators and for end users as part of the cloud service, the cloud service provider separates these interfaces from one another and ensures that access paths for customer administrators differ from those for end users.	Functional	Intersects With	Network Device Plane Segmentation	NET-09	Automated mechanisms exist to separate network appliance functions (e.g., management, control and data planes) to prevent ordinary traffic from accessing functions that: (1) Manage network appliances; and/or (2) Affect network operations.	3		NET-06.8
IAM-08.01B	Authentication Mechanisms	System components in the cloud service provider's area of responsibility that are used to provide the cloud service authenticate users of the cloud service provider's internal and external personnel as well as system components that are involved in the cloud service provider's automated authorisation processes.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-32	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	8		IAC-02
IAM-08.01B	Authentication Mechanisms	System components in the cloud service provider's area of responsibility that are used to provide the cloud service authenticate users of the cloud service provider's internal and external personnel as well as system components that are involved in the cloud service provider's automated authorisation processes.	Functional	Intersects With	Identification & Authentication for Devices	IAC-34	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	3		IAC-04
IAM-08.02B	Authentication Mechanisms	The cloud service provider enforces multi-factor authentication (MFA) for all access to the production environment. This requirement applies to both human users and automated processes, ensuring that only authorised entities can access systems and data in the production environment.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	8		IAC-06
IAM-08.03B	Authentication Mechanisms	Within the production environment, user authentication takes place through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security. If digitally signed certificates are used, administration is carried out in accordance with the policies and procedures for the use of cryptographic mechanisms (cf. CRY-01).	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
IAM-08.03B	Authentication Mechanisms	Within the production environment, user authentication takes place through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security. If digitally signed certificates are used, administration is carried out in accordance with the policies and procedures for the use of cryptographic mechanisms (cf. CRY-01).	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
IAM-08.04B	Authentication Mechanisms	The authentication requirements are derived from a risk assessment and documented, communicated and provided in an authentication policy according to SP-01. Compliance with the requirements is enforced by the configuration of the system components, as far as technically possible. The authentication policy describes at least the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
IAM-08.04B	Authentication Mechanisms	The authentication requirements are derived from a risk assessment and documented, communicated and provided in an authentication policy according to SP-01. Compliance with the requirements is enforced by the configuration of the system components, as far as technically possible. The authentication policy describes at least the following aspects:	Functional	Intersects With	Identification & Authentication Policy	IAC-01	Mechanisms exist to establish a formal, documented identification and authentication policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and	8		
IAM-08.04B	Authentication Mechanisms	The authentication requirements are derived from a risk assessment and documented, communicated and provided in an authentication policy according to SP-01. Compliance with the requirements is enforced by the configuration of the system components, as far as technically possible. The authentication policy describes at least the following aspects:	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5		IAC-10
IAM-08.04B.1	Authentication Mechanisms	The selection of appropriate mechanisms for every level of risk and each identity type;	Functional	Intersects With	Adaptive Identification & Authentication	IAC-41	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.	5		IAC-13
IAM-08.04B.2	Authentication Mechanisms	The protection of credentials that the authentication mechanisms use, including the confidentiality of personal or shared authentication information and non-sharing of credentials;	Functional	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5		IAC-10.5
IAM-08.04B.2	Authentication Mechanisms	The protection of credentials that the authentication mechanisms use, including the confidentiality of personal or shared authentication information and non-sharing of credentials;	Functional	Intersects With	Credential Sharing	IAC-23	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	3		IAC-19
IAM-08.04B.3	Authentication Mechanisms	The generation and distribution of credentials for any new identity;	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5		IAC-10
IAM-08.04B.4	Authentication Mechanisms	The non-reuse of credentials;	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
IAM-08.04B.5	Authentication Mechanisms	Rules on the storage of credentials;	Functional	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5		IAC-10.5
IAM-08.04B.6	Authentication Mechanisms	Rules for renewing credentials, including periodic renewals and renewals in case a credential is lost or compromised; and	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5		IAC-10
IAM-08.04B.7	Authentication Mechanisms	Rules on the required strength of credentials, including trade-offs between entropy and ability to memorise where applicable, as well as mechanisms for communicating and enforcing these rules.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
IAM-08.05B	Authentication Mechanisms	The cloud service provider determines by means of a risk assessment (cf. OIS-07) the risk that the authentication mechanisms integrated into the system components under its responsibility used to provide the cloud service become outdated. Based on the results of the risk assessment, the cloud service provider implements appropriate measures for exchanging outdated authentication mechanisms or the system components into which they are integrated.	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	3		IAC-10
IAM-08.05B	Authentication Mechanisms	The cloud service provider determines by means of a risk assessment (cf. OIS-07) the risk that the authentication mechanisms integrated into the system components under its responsibility used to provide the cloud service become outdated. Based on the results of the risk assessment, the cloud service provider implements appropriate measures for exchanging outdated authentication mechanisms or the system components into which they are integrated.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
IAM-08.06B	Authentication Mechanisms	Any authentication mechanism integrated into the system components used to provide the cloud service has a mechanism for disabling an identity after a predefined number of unsuccessful authentication attempts.	Functional	Intersects With	Account Lockout	CFG-04.1	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	8		IAC-22
IAM-08.07B	Authentication Mechanisms	The cloud service provider implements measures which require that users can only access non-personal identities assigned to multiple persons after they have already been authenticated with their identity assigned to a single person.	Functional	Intersects With	Credential Sharing	IAC-23	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5		IAC-19
IAM-08.07B	Authentication Mechanisms	The cloud service provider implements measures which require that users can only access non-personal identities assigned to multiple persons after they have already been authenticated with their identity assigned to a single person.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-32	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	3		IAC-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
IAM-08.02AS	Authentication Mechanisms	IAM-08.02AS, sharpening IAM-08.02B The cloud service provider enforces multi-factor authentication (MFA) for all access to any environment. This requirement applies to both human users and automated processes, ensuring that only authorised entities can access systems and data in all of the environments.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	8		IAC-06
IAM-08.03AS	Authentication Mechanisms	IAM-08.03AS, sharpening IAM-08.03B Within an environment, user authentication takes place through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security. If digitally signed certificates are used, administration is carried out in accordance with the policies and procedures for the use of cryptographic mechanisms (cf. CRY-01).	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
IAM-08.03AS	Authentication Mechanisms	IAM-08.03AS, sharpening IAM-08.03B Within an environment, user authentication takes place through passwords, digitally signed certificates or procedures that achieve at least an equivalent level of security. If digitally signed certificates are used, administration is carried out in accordance with the policies and procedures for the use of cryptographic mechanisms (cf. CRY-01).	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
IAM-09.01B	Confidentiality of Authentication Information	The allocation of authentication information to access system components used to provide the cloud service to internal and external users of the cloud service provider and system components that are involved in automated authorisation processes of the cloud service provider is done in an orderly manner that ensures the confidentiality of the information.	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5		IAC-10
IAM-09.01B	Confidentiality of Authentication Information	The allocation of authentication information to access system components used to provide the cloud service to internal and external users of the cloud service provider and system components that are involved in automated authorisation processes of the cloud service provider is done in an orderly manner that ensures the confidentiality of the information.	Functional	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	3		IAC-10.5
IAM-09.02B	Confidentiality of Authentication Information	Authentication credentials are managed with a security level that matches or exceeds the classification of the system component they protect.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	3		DCH-02
IAM-09.02B	Confidentiality of Authentication Information	Authentication credentials are managed with a security level that matches or exceeds the classification of the system component they protect.	Functional	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5		IAC-10.5
IAM-09.03B	Confidentiality of Authentication Information	If passwords are used as authentication information, their confidentiality is ensured by the following procedures, as far as technically possible:	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
IAM-09.03B.1	Confidentiality of Authentication Information	Users can initially create the password themselves or shall change an initial password when logging on to the system component for the first time. An initial password loses its validity after a maximum of 14 days;	Functional	Intersects With	Default Authenticators	IAC-14.4	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5		IAC-10.8
IAM-09.03B.2	Confidentiality of Authentication Information	When creating passwords, compliance with the authentication policy (cf. IAM-08) is enforced as far as technically possible;	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
IAM-09.03B.3	Confidentiality of Authentication Information	The user is informed about changing or resetting the password; and	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	3		IAC-10
IAM-09.03B.4	Confidentiality of Authentication Information	The server-side storage takes place using state of the art cryptographic hash functions, with the exception of passwords that are stored in the plain text form for later use, for example in a password manager. In this case, state of the art cryptographic mechanisms are used to protect the passwords.	Functional	Intersects With	Cryptographic Hash	CRY-14	Mechanisms exist to utilize hash algorithms to generate a hash value that can be used to validate the integrity of data and/or software.	3		CRY-13
IAM-09.03B.4	Confidentiality of Authentication Information	The server-side storage takes place using state of the art cryptographic hash functions, with the exception of passwords that are stored in the plain text form for later use, for example in a password manager. In this case, state of the art cryptographic mechanisms are used to protect the passwords.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
IAM-09.04B	Confidentiality of Authentication Information	Deviations are evaluated by means of a risk assessment according to OIS-07 and mitigating measures derived from this are implemented.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
IAM-09.04B	Confidentiality of Authentication Information	Deviations are evaluated by means of a risk assessment according to OIS-07 and mitigating measures derived from this are implemented.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	3		RSK-06.2
IAM-09.05B	Confidentiality of Authentication Information	Rules and recommendations for managing credentials in accordance with the authentication policy (cf. IAM-08) are documented, communicated and made available to all users under the responsibility of the cloud service provider. They include recommendations on password managers and recommendations to specifically address classical attacks such as phishing, social attacks, and whaling.	Functional	Intersects With	User Responsibilities for Account Management	IAC-22	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards and certificates).	5		IAC-18
IAM-09.05B	Confidentiality of Authentication Information	Rules and recommendations for managing credentials in accordance with the authentication policy (cf. IAM-08) are documented, communicated and made available to all users under the responsibility of the cloud service provider. They include recommendations on password managers and recommendations to specifically address classical attacks such as phishing, social attacks, and whaling.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3		SAT-02
IAM-09.06B	Confidentiality of Authentication Information	Used cryptographic mechanisms comply with the policies and instructions for cryptographic mechanisms (cf. CRY-01).	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic	5		CRY-01
IAM-09.06B	Confidentiality of Authentication Information	Used cryptographic mechanisms comply with the policies and instructions for cryptographic mechanisms (cf. CRY-01).	Functional	Intersects With	Cryptographic Module Authentication	IAC-38	Automated mechanisms exist to enable Technology Assets, Applications and/or Services (TAAS) to authenticate to a cryptographic module.	5		IAC-12
IAM-09.07B	Confidentiality of Authentication Information	Password reset procedures are valid for at most 24 hours. After the reset procedure has been used, the password is to be changed by the user.	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	3		IAC-10
IAM-09.01AC	Confidentiality of Authentication Information	The users sign a declaration in which they assure that they treat personal (or shared) authentication information confidentially and keep it exclusively for themselves (within the members of the group).	Functional	Intersects With	User Responsibilities for Account Management	IAC-22	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards and	5		IAC-18
IAM-09.01AC	Confidentiality of Authentication Information	The users sign a declaration in which they assure that they treat personal (or shared) authentication information confidentially and keep it exclusively for themselves (within the members of the group).	Functional	Intersects With	Credential Sharing	IAC-23	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	3		IAC-19
5.8	Cryptography and Key Management (CRY)	Objective: Ensure appropriate and effective use of cryptography to protect the confidentiality, authenticity or integrity of information.	Functional	No Relationship	N/A	N/A	N/A	0		
CRY-01.01B	Policy for the Use of Cryptographic Mechanisms	Policies and procedures with procedures and technical safeguards for cryptographic mechanisms are documented, communicated and provided according to SP-01, in which the following aspects are described:	Functional	Subset Of	Cryptographic Protections Policy	CRY-01	Mechanisms exist to establish a formal, documented cryptographic protections policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving	10		
CRY-01.01B	Policy for the Use of Cryptographic Mechanisms	Policies and procedures with procedures and technical safeguards for cryptographic mechanisms are documented, communicated and provided according to SP-01, in which the following aspects are described:	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	8		CRY-01

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
CRY-01.01B	Policy for the Use of Cryptographic Mechanisms	Policies and procedures with procedures and technical safeguards for cryptographic mechanisms are documented, communicated and provided according to SP-01, in which the following aspects are described:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
CRY-01.01B.1	Policy for the Use of Cryptographic Mechanisms	Usage of encryption procedures and secure network protocols that correspond to the state of the art;	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic	5		CRY-01
CRY-01.01B.1	Policy for the Use of Cryptographic Mechanisms	Usage of encryption procedures and secure network protocols that correspond to the state of the art;	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-37	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive and/or regulated data during transmission over open, public networks.	3		NET-12
CRY-01.01B.2	Policy for the Use of Cryptographic Mechanisms	Usage of hash functions and salt values, that both correspond to the state of the art;	Functional	Intersects With	Cryptographic Hash	CRY-14	Mechanisms exist to utilize hash algorithms to generate a hash value that can be used to validate the integrity of data and/or software.	5		CRY-13
CRY-01.01B.3	Policy for the Use of Cryptographic Mechanisms	Usage of signature schemes that correspond to the state of the art;	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic	5		CRY-01
CRY-01.01B.4	Policy for the Use of Cryptographic Mechanisms	Risk-based provisions for the use of encryption and authentication which are aligned with the information classification schemes (cf. AM-09) and consider the communication channel, type, strength and quality of the encryption;	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01
CRY-01.01B.4	Policy for the Use of Cryptographic Mechanisms	Risk-based provisions for the use of encryption and authentication which are aligned with the information classification schemes (cf. AM-09) and consider the communication channel, type, strength and quality of the encryption;	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	3		DCH-02
CRY-01.01B.5	Policy for the Use of Cryptographic Mechanisms	Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal, backup, restoration and deletion of the keys;	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	8		CRY-09
CRY-01.01B.6	Policy for the Use of Cryptographic Mechanisms	Requirements for the rotation of cryptographic keys that follow industry best practices and consider the potential risk of information exposure;	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-01.01B.7	Policy for the Use of Cryptographic Mechanisms	Consideration of relevant legal and regulatory obligations and requirements;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
CRY-01.01B.7	Policy for the Use of Cryptographic Mechanisms	Consideration of relevant legal and regulatory obligations and requirements;	Functional	Subset Of	Cryptographic Protections Policy	CRY-01	Mechanisms exist to establish a formal, documented cryptographic protections policy that: (1) Conveys executive management's intent;	10		
CRY-01.01B.7	Policy for the Use of Cryptographic Mechanisms	Consideration of relevant legal and regulatory obligations and requirements;	Functional	Intersects With	Export-Controlled Cryptography	CRY-15	Mechanisms exist to address the exporting of cryptographic technologies in compliance with relevant statutory and regulatory requirements.	3		CRY-01.2
CRY-01.01B.8	Policy for the Use of Cryptographic Mechanisms	Documentation of a change management process for managing cryptographic, encryption, authentication and key management technology changes; and	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	5		CHG-01
CRY-01.01B.8	Policy for the Use of Cryptographic Mechanisms	Documentation of a change management process for managing cryptographic, encryption, authentication and key management technology changes; and	Functional	Subset Of	Cryptographic Protections Policy	CRY-01	Mechanisms exist to establish a formal, documented cryptographic protections policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving	10		
CRY-01.01B.9	Policy for the Use of Cryptographic Mechanisms	Consideration of crypto-agility to allow for efficient substitution of implemented cryptographic mechanisms during their intended lifetimes.	Functional	Intersects With	Crypto-Agility Architecture	QTS-09	Mechanisms exist to validate design-level cryptographic agility across protocols, libraries, kernels and hardware to ensure Technology Assets, Applications and/or Services (TAAS) can support larger Post-Quantum Cryptography (PQC) key, signature and ciphertext sizes.	5		QTS-06
CRY-01.02B	Policy for the Use of Cryptographic Mechanisms	Reviews of policies and procedures regarding cryptographic mechanisms include checks that the policies and procedures are up to date and comply with the BSI technical guideline (BSI TR-02102) or suitable NIST guidelines (e.g. FIPS 140 series and SP 800 series). Deviations are analysed and documented in a risk assessment for cryptographic mechanisms valid at the given time. Remediation measures are to be taken based on risk.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5		CRY-01
CRY-01.02B	Policy for the Use of Cryptographic Mechanisms	Reviews of policies and procedures regarding cryptographic mechanisms include checks that the policies and procedures are up to date and comply with the BSI technical guideline (BSI TR-02102) or suitable NIST guidelines (e.g. FIPS 140 series and SP 800 series). Deviations are analysed and documented in a risk assessment for cryptographic mechanisms valid at the given time. Remediation measures are to be taken based on risk.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8		GOV-03
CRY-01.01AC	Policy for the Use of Cryptographic Mechanisms	The cloud service provider has defined and documented a Post-Quantum-Cryptography (PQC) strategy according to SP-01 to address threats posed by adversaries in possession of a quantum computer.	Functional	Intersects With	Quantum Security Policy	QTS-01	Mechanisms exist to establish a formal, documented quantum security policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving risks, threats and other changes that affect the organization.	5		QTS-01.1
CRY-01.01AC	Policy for the Use of Cryptographic Mechanisms	The cloud service provider has defined and documented a Post-Quantum-Cryptography (PQC) strategy according to SP-01 to address threats posed by adversaries in possession of a quantum computer.	Functional	Intersects With	Post-Quantum Cryptography Agility Plan (PQCAP)	QTS-06	Mechanisms exist to develop a risk-prioritized Post-Quantum Cryptography Agility Plan (PQCAP) that: (1) Enables cryptographic agility; (2) Aligns with evolving security standards; and (3) Defines the approach for selecting and implementing PQC algorithms.	8		QTS-03
CRY-01.02AC	Policy for the Use of Cryptographic Mechanisms	The cloud service provider's PQC strategy is aligned with cryptography policies and procedures and includes the following aspects:	Functional	Intersects With	Post-Quantum Cryptography Agility Plan (PQCAP)	QTS-06	Mechanisms exist to develop a risk-prioritized Post-Quantum Cryptography Agility Plan (PQCAP) that: (1) Enables cryptographic agility; (2) Aligns with evolving security standards; and (3) Defines the approach for selecting and implementing PQC algorithms.	5		QTS-03
CRY-01.02AC.1	Policy for the Use of Cryptographic Mechanisms	Maintenance of an inventory of cryptographic mechanisms in use, including priority levels to each inventory item based on the impact and probabilities of the risks posed by quantum computing attacks and the effort to remediate such risks;	Functional	Intersects With	Data Shelf-Life Classification for Post-Quantum Cryptography (PQC) Prioritization	QTS-03	Mechanisms exist to classify Technology Assets, Applications, Services and Data (TAASD) by confidentiality shelf-life and use that classification as a direct input to Post-Quantum Cryptography (PQC) migration prioritization, including prioritizing data with a shelf-life exceeding the expected PQC arrival horizon.	3		QTS-01.2
CRY-01.02AC.1	Policy for the Use of Cryptographic Mechanisms	Maintenance of an inventory of cryptographic mechanisms in use, including priority levels to each inventory item based on the impact and probabilities of the risks posed by quantum computing attacks and the effort to remediate such risks;	Functional	Intersects With	Post-Quantum Cryptography (PQC) Asset Inventory	QTS-07.1	Mechanisms exist to maintain a current inventory of cryptographic assets that includes: (1) Algorithms (asymmetric and symmetric); (2) Key lengths; (3) Libraries; (4) Protocols; (5) Associated Technology Assets, Applications and/or Services (TAAS) utilizing the cryptography; and (6) Federal Information Processing Standards (FIPS) validation status from the Cryptographic Module Validation Program (CMVP), including certificate number, if applicable.	8		QTS-04.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
CRY-01.02AC.2	Policy for the Use of Cryptographic Mechanisms	Staying informed about encryption measures that are deemed state of the art and secure against adversaries who possess a quantum computer;	Functional	Intersects With	Quantum Threat Intelligence Monitoring	QTS-08	Mechanisms exist to maintain an ongoing quantum threat intelligence function that monitors: (1) Cryptanalytic threat developments; (2) Quantum computing capability advances; and (3) NIST and/or regulatory updates to approved algorithm lists.	8		QTS-05.1
CRY-01.02AC.3	Policy for the Use of Cryptographic Mechanisms	Usage of hybrid cryptography models to ensure security for both quantum and non-quantum computing based attacks; and	Functional	Intersects With	Hybrid / Composite Cryptography	QTS-09.9	Mechanisms exist to leverage hybrid/composite algorithms as a transition path to Post-Quantum Cryptography (PQC) solutions that: (1) Support hybrid signatures (e.g., ECDSA + ML-DSA) and hybrid Key Encapsulation Mechanisms (KEMs) (e.g., ECDH + ML-KEM); (2) Ensure certificate formats, Public Key Infrastructure (PKI) and trust anchors can support dual-key or dual-certificate models; and (3) Plan for eventual removal of classical algorithms once PQC confidence is sufficient.	8		QTS-06.9
CRY-01.02AC.4	Policy for the Use of Cryptographic Mechanisms	Definition of trigger events, required resources, transition plans and success criteria for implementation of post-quantum cryptographic mechanisms.	Functional	Intersects With	Post-Quantum Cryptography (PQC) Transition Planning & Hybrid Mode Support	QTS-06.1	Mechanisms exist to allocate resources to: (1) Transition legacy Technology Assets, Applications and/or Services (TAAS) to Post-Quantum Cryptography (PQC) algorithms; and (2) Support hybrid cryptography during a defined transition period.	8		QTS-03.1
CRY-01.03AC	Policy for the Use of Cryptographic Mechanisms	The PQC strategy, including the inventory and risk assessment, is reviewed at least annually or in case of significant changes impacting the PQC strategy.	Functional	Intersects With	Cryptographic Agility Risk Assessment (CARA)	QTS-04	Mechanisms exist to perform a Cryptographic Agility Risk Assessment (CARA) that analyzes Technology Assets, Applications, Services and Data (TAASD) to: (1) Identify TAASD most vulnerable to quantum-enabled cryptanalytic threats; and (2) Prioritize TAASD based on potential business impact.	3		QTS-02
CRY-01.03AC	Policy for the Use of Cryptographic Mechanisms	The PQC strategy, including the inventory and risk assessment, is reviewed at least annually or in case of significant changes impacting the PQC strategy.	Functional	Intersects With	Post-Quantum Cryptography Agility Plan (PQCAP)	QTS-06	Mechanisms exist to develop a risk-prioritized Post-Quantum Cryptography Agility Plan (PQCAP) that: (1) Enables cryptographic agility; (2) Aligns with evolving security standards; and (3) Defines the approach for selecting and implementing PQC algorithms.	5		QTS-03
CRY-02.01B	Cryptographic Change Management	When implementing changes to cryptographic systems, the cloud service provider performs an evaluation of their potential impact in accordance with DEV-06. This process includes an analysis of the cloud infrastructure of the cloud service, as well as an analysis of potential disruptions to cloud service customer-managed workloads and the evaluation of residual risks, cost implications, and integration benefits. The cloud service provider informs cloud service customers of these downstream effects to prevent unforeseen failures within the cloud service customer's specific cryptographic implementations.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5		CHG-03
CRY-02.01B	Cryptographic Change Management	When implementing changes to cryptographic systems, the cloud service provider performs an evaluation of their potential impact in accordance with DEV-06. This process includes an analysis of the cloud infrastructure of the cloud service, as well as an analysis of potential disruptions to cloud service customer-managed workloads and the evaluation of residual risks, cost implications, and integration benefits. The cloud service provider informs cloud service customers of these downstream effects to prevent unforeseen failures within the cloud service customer's specific cryptographic implementations.	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	3		CRY-01
CRY-02.02B	Cryptographic Change Management	All changes and adjustments to cryptographic systems are documented and traceable.	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	5		CHG-02
CRY-02.03B	Cryptographic Change Management	The personnel responsible for cryptographic systems is regularly trained and informed about respective changes.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03
CRY-03.01B	Review of Cryptography Practices	The cloud service provider ensures that encryption, authentication and key management practices are regularly audited in accordance with COM-02 and COM-03 to identify and address potential vulnerabilities. At a minimum, reviews are performed annually and immediately following security incidents involving cryptographic components.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5		CPL-03.2
CRY-03.01B	Review of Cryptography Practices	The cloud service provider ensures that encryption, authentication and key management practices are regularly audited in accordance with COM-02 and COM-03 to identify and address potential vulnerabilities. At a minimum, reviews are performed annually and immediately following security incidents involving cryptographic components.	Functional	Intersects With	Cryptographic Cipher Suites and Protocols Inventory	CRY-04	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.	5		CRY-01.5
CRY-03.02B	Review of Cryptography Practices	As part of the reviews, the cloud service provider determines if the cryptographic practices align with the state of the art and updates them as needed.	Functional	Intersects With	Cryptographic Cipher Suites and Protocols Inventory	CRY-04	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.	5		CRY-01.5
CRY-04.01B	Protection of Data for Transmission (Transport Protection)	The cloud service provider has established procedures and technical safeguards for state of the art encryption and authentication for the transmission of cloud service customer data and cloud service derived data over public networks.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	8		CRY-03
CRY-04.01B	Protection of Data for Transmission (Transport Protection)	The cloud service provider has established procedures and technical safeguards for state of the art encryption and authentication for the transmission of cloud service customer data and cloud service derived data over public networks.	Functional	Intersects With	Integrity of Data In Transit	CRY-06	Cryptographic mechanisms exist to detect unauthorized changes to data in transit.	5		CRY-04
CRY-04.02B	Protection of Data for Transmission (Transport Protection)	During remote access to the production environment, the cloud service provider uses state of the art cryptographic mechanisms, including personnel authentication, to protect the communication.	Functional	Intersects With	Non-Console Administrative Access	CFG-04.7	Cryptographic mechanisms exist to protect the confidentiality and integrity of non-console administrative access.	5		CRY-06
CRY-04.02B	Protection of Data for Transmission (Transport Protection)	During remote access to the production environment, the cloud service provider uses state of the art cryptographic mechanisms, including personnel authentication, to protect the communication.	Functional	Intersects With	Remote Access Cryptographic Protections	NET-26.5	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	5		NET-14.2
CRY-04.01AS	Protection of Data for Transmission (Transport Protection)	CRY-04.01AS, sharpening CRY-04.01B The cloud service provider has established procedures and technical safeguards for state of the art encryption and authentication for the transmission of all data.	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	8		CRY-03
CRY-04.01AS	Protection of Data for Transmission (Transport Protection)	CRY-04.01AS, sharpening CRY-04.01B The cloud service provider has established procedures and technical safeguards for state of the art encryption and authentication for the transmission of all data.	Functional	Intersects With	Integrity of Data In Transit	CRY-06	Cryptographic mechanisms exist to detect unauthorized changes to data in transit.	5		CRY-04
CRY-05.01B	Encryption of Sensitive Data at Rest	The cloud service provider has established procedures and technical safeguards to encrypt cloud service customer data during storage (i.e. at rest).	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	8		CRY-05
CRY-05.02B	Encryption of Sensitive Data at Rest	In general, the private keys (for asymmetric algorithms) or secret keys (for symmetric algorithms) used for encryption are accessible only by the cloud service customer in accordance with applicable legal and regulatory obligations and requirements. If due to the nature of the cloud service, the cloud service provider has to access the private or secret keys of the customer in order to provide the cloud service, this access is performed in accordance with IAM-07. Exceptions follow a specified procedure.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-05.02B	Encryption of Sensitive Data at Rest	In general, the private keys (for asymmetric algorithms) or secret keys (for symmetric algorithms) used for encryption are accessible only by the cloud service customer in accordance with applicable legal and regulatory obligations and requirements. If due to the nature of the cloud service, the cloud service provider has to access the private or secret keys of the customer in order to provide the cloud service, this access is performed in accordance with IAM-07. Exceptions follow a specified procedure.	Functional	Intersects With	External System Cryptographic Key Control	CRY-10.7	Mechanisms exist to maintain control of cryptographic keys for encrypted material stored or transmitted through an external system.	5		CRY-09.7

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
CRY-05.03B	Encryption of Sensitive Data at Rest	The procedures for the use of private keys, including any exceptions, are agreed with the cloud service customer.	Functional	Intersects With	Third-Party Cryptographic Keys	CRY-10.6	Mechanisms exist to ensure customers are provided with appropriate key management guidance whenever cryptographic keys are shared.	5		CRY-09.6
CRY-05.04B	Encryption of Sensitive Data at Rest	If any changes of these procedures and technical safeguards may affect the confidentiality of the cloud service customer data, the cloud service provider communicates these changes to the cloud service	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		CHG-05
CRY-05.05B	Encryption of Sensitive Data at Rest	If the cloud service provider uses a master key, the cloud service provider regularly tests the suitability of the design and operating effectiveness of the respective controls.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-05.05B	Encryption of Sensitive Data at Rest	If the cloud service provider uses a master key, the cloud service provider regularly tests the suitability of the design and operating effectiveness of the respective controls.	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	3		IAO-02
CRY-05.01AC	Encryption of Sensitive Data at Rest	The cloud service provider ensures that secure encryption mechanisms are in place to prevent the recovery of cloud service customer data when resources are reallocated or physical media are recovered.	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	3		CRY-05
CRY-05.01AC	Encryption of Sensitive Data at Rest	The cloud service provider ensures that secure encryption mechanisms are in place to prevent the recovery of cloud service customer data when resources are reallocated or physical media are recovered.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5		DCH-09
CRY-06.01B	Secure Key Generation	Procedures and technical safeguards for the secure generation of keys for different cryptographic systems and applications are documented and implemented. These safeguards require the use of secure random bit generators or generation based on keys that were created in this fashion.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-06.01B	Secure Key Generation	Procedures and technical safeguards for the secure generation of keys for different cryptographic systems and applications are documented and implemented. These safeguards require the use of secure random bit generators or generation based on keys that were created in this fashion.	Functional	Intersects With	Entropy Source & Random Bit Generation	QTS-09.1	Mechanisms exist to use validated entropy sources and random bit generators that comply with NIST SP 800-90B to support Post-Quantum Cryptography (PQC): (1) Key generation; (2) Nonce generation; (3) Probabilistic algorithm inputs; and (4) Key validation.	5		QTS-06.1
CRY-07.01B	Rotation of Cryptographic Keys	The cloud service provider has established a schedule for rotating cryptographic keys that aligns with the requirements for cryptographic key rotation established in CRY-01. If, based on the results of a risk assessment, the cloud service provider does not perform key rotation, this decision is transparently communicated to the customer.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-08.01B	Public-Key Certificate Issuance	The cloud service provider has documented and implemented procedures to securely issue and obtain public-key certificates, ensuring the integrity and authenticity of cryptographic keys. These procedures include:	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-09	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	8		CRY-08
CRY-08.01B.1	Public-Key Certificate Issuance	Verification of identity before issuing public-key certificates that are issued by or on behalf of the cloud service provider for its own system components or personnel to ensure they are granted to legitimate entities;	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-09	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5		CRY-08
CRY-08.01B.1	Public-Key Certificate Issuance	Verification of identity before issuing public-key certificates that are issued by or on behalf of the cloud service provider for its own system components or personnel to ensure they are granted to legitimate entities;	Functional	Intersects With	Identity Proofing (Identity Verification)	IAC-05	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	3		IAC-28
CRY-08.01B.2	Public-Key Certificate Issuance	Secure methods for issuing certificates that are issued by or on behalf of the cloud service provider for its own system components or personnel to prevent unauthorised access; and	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-09	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service	5		CRY-08
CRY-08.01B.3	Public-Key Certificate Issuance	Procedures for obtaining public-key certificates from trusted Certificate Authorities to ensure the authenticity of the certificates used by the cloud service provider.	Functional	Intersects With	Certificate Authorities	CRY-12	Automated mechanisms exist to enable the use of organization-defined Certificate Authorities (CAs) to facilitate the establishment of protected sessions.	5		CRY-11
CRY-09.01B	Secure Key Provisioning	The cloud service provider has documented and implemented procedures and technical safeguards to ensure that cryptographic keys are provisioned and activated securely within its area of responsibility. These procedures include the verification of identity and authorisation before provisioning and activating keys to ensure they are granted to legitimate entities.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-09.01B	Secure Key Provisioning	The cloud service provider has documented and implemented procedures and technical safeguards to ensure that cryptographic keys are provisioned and activated securely within its area of responsibility. These procedures include the verification of identity and authorisation before provisioning and activating keys to ensure they are granted to legitimate entities.	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-10.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5		CRY-09.4
CRY-09.02B	Secure Key Provisioning	Provisioned keys include activation and deactivation dates to ensure that their use is time limited.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-10.01B	Secure Storage of Keys	The cloud service provider has documented and implemented technical safeguards for the secure storage of cryptographic keys. This includes ensuring separation of the key management system from the application and middleware layers, defining how authorised users gain access and addressing the geographic residency of keys to comply with contractual, legal, regulatory, and security requirements.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-10.01B	Secure Storage of Keys	The cloud service provider has documented and implemented technical safeguards for the secure storage of cryptographic keys. This includes ensuring separation of the key management system from the application and middleware layers, defining how authorised users gain access and addressing the geographic residency of keys to comply with contractual, legal, regulatory, and security requirements.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	3		CLD-09
CRY-10.01AC	Secure Storage of Keys	Based on a risk assessment (cf. OIS-07), the cloud service provider uses a suitable software or hardware security module for the secure storage of cryptographic keys.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-11.01B	Cryptographic Key Archival	The cloud service provider has documented and implemented procedures and technical safeguards for the secure archiving of cryptographic keys. These include:	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-11.01B.1	Cryptographic Key Archival	Storage of archived keys in a repository to prevent unauthorised access;	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-11.01B.2	Cryptographic Key Archival	Restriction of access to archived keys to authorised personnel based on the principle of least privilege;	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-11.01B.2	Cryptographic Key Archival	Restriction of access to archived keys to authorised personnel based on the principle of least privilege;	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business	3		IAC-21
CRY-11.01B.3	Cryptographic Key Archival	Support of later recovery of information through archived keys;	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-10.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5		CRY-09.3
CRY-11.01B.4	Cryptographic Key Archival	Retention of archived keys only for as long as needed and secure destruction afterwards; and	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-11.01B.4	Cryptographic Key Archival	Retention of archived keys only for as long as needed and secure destruction afterwards; and	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	3		DCH-21

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
CRY-11.01B.5	Cryptographic Key Archival	Logging of all activities related to the storage and recovery of archived keys.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
CRY-12.01B	Cryptographic Key Transition Management	The cloud service provider has documented and implemented procedures to oversee the transition of cryptographic keys, including their movement into and out of suspension. These procedures ensure that all key transitions are thoroughly monitored, reviewed, and approved to maintain security and comply with applicable laws and regulations.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-13.01B	Handling of Compromised Keys	The cloud service provider manages the use of compromised cryptographic keys to ensure they are only used in controlled circumstances and solely for decryption or verification (in case of signature keys), while complying with legal and regulatory	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-13.02B	Handling of Compromised Keys	The cloud service provider notifies affected cloud service customers without undue delay that their keys have been compromised and will no longer be used for encryption or signing.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
CRY-14.01B	Secure Deactivation of Cryptographic Keys	The cloud service provider has documented and implemented procedures to deactivate cryptographic keys. These procedures ensure that:	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-14.01B.1	Secure Deactivation of Cryptographic Keys	Expired keys are no longer used for encryption purposes, but may still be used for decryption if necessary;	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-14.01B.2	Secure Deactivation of Cryptographic Keys	Expired keys are no longer used for signature creation, but may still be used for signature verification;	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-14.01B.3	Secure Deactivation of Cryptographic Keys	Deactivated keys are eventually destroyed when they are no longer required, with relevant metadata retained for auditing; and	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-14.01B.3	Secure Deactivation of Cryptographic Keys	Deactivated keys are eventually destroyed when they are no longer required, with relevant metadata retained for auditing; and	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	3		DCH-21
CRY-14.01B.4	Secure Deactivation of Cryptographic Keys	All actions related to key deactivation and destruction are recorded in the key management system to maintain a detailed audit log.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
CRY-15.01B	Requirements for Pre-Shared Keys	If pre-shared keys or wildcard certificates are used, the cloud service provider has documented and implemented dedicated procedures and technical safeguards to ensure their secure use and provisioning.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-15.01B	Requirements for Pre-Shared Keys	If pre-shared keys or wildcard certificates are used, the cloud service provider has documented and implemented dedicated procedures and technical safeguards to ensure their secure use and provisioning.	Functional	Intersects With	Certificate Monitoring	CRY-13	Automated mechanisms exist to discover when new certificates are issued for organization-controlled domains.	3		CRY-12
CRY-16.01B	Operational Continuity for Key Management	The cloud service provider has assessed the balance between conducting backups of key material stored in a Hardware Security Module (HSM) for key restoration and building redundancy or comparable measures for securing keys to ensure operational continuity. This assessment includes evaluating the risk of key exposure if control over the key material is lost. Decisions regarding whether to use the backups of keys or to establish redundancy are documented, and the chosen measures are reviewed for their effectiveness and compliance with contractual, legal and regulatory	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
CRY-16.01B	Operational Continuity for Key Management	The cloud service provider has assessed the balance between conducting backups of key material stored in a Hardware Security Module (HSM) for key restoration and building redundancy or comparable measures for securing keys to ensure operational continuity. This assessment includes evaluating the risk of key exposure if control over the key material is lost. Decisions regarding whether to use the backups of keys or to establish redundancy are documented, and the chosen measures are reviewed for their effectiveness and compliance with contractual, legal and regulatory	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-10.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5		CRY-09.3
CRY-16.02B	Operational Continuity for Key Management	Procedures for the recovery of lost or corrupted keys are in place.	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-10.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	8		CRY-09.3
CRY-17.01B	Cryptographic Key Lifecycle Management	The cloud service provider has documented and implemented procedures and technical safeguards to monitor and document the lifecycle of cryptographic keys and materials.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-17.01B	Cryptographic Key Lifecycle Management	The cloud service provider has documented and implemented procedures and technical safeguards to monitor and document the lifecycle of cryptographic keys and materials.	Functional	Intersects With	Cryptographic Bill of Materials (CBOM)	TDA-21.1	Mechanisms exist to develop and maintain a Cryptographic Bill of Materials (CBOM) by analyzing the organization's cryptographic architecture, including: (1) Hardware; (2) Firmware; (3) Software modules; and (4) Communication protocols.	3		QTS-04.2
CRY-17.02B	Cryptographic Key Lifecycle Management	For all keys except for ephemeral keys, the aforementioned safeguards ensure detailed records of each key from creation to destruction, including any status changes.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
CRY-18.01B	Usage of External Key Management Systems	In the case that external key management systems (KMS) are integrated into the service, the cloud service provider ensures that the procedures and technical safeguards for the usage of external key management systems (KMS) are established. The following aspects are taken into account:	Functional	Intersects With	External System Cryptographic Key Control	CRY-10.7	Mechanisms exist to maintain control of cryptographic keys for encrypted material stored or transmitted through an external system.	5		CRY-09.7
CRY-18.01B	Usage of External Key Management Systems	In the case that external key management systems (KMS) are integrated into the service, the cloud service provider ensures that the procedures and technical safeguards for the usage of external key management systems (KMS) are established. The following aspects are taken into account:	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-04
CRY-18.01B.1	Usage of External Key Management Systems	The external KMS have recognised security certifications that reflect the state of the art to comply with legal, regulatory and contractual requirements;	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5		TPM-05.8
CRY-18.01B.2	Usage of External Key Management Systems	The integration of the external KMS into the cloud infrastructure is secure to ensure the confidentiality, integrity, and availability of the keys;	Functional	Intersects With	External System Cryptographic Key Control	CRY-10.7	Mechanisms exist to maintain control of cryptographic keys for encrypted material stored or transmitted through an external system.	5		CRY-09.7
CRY-18.01B.3	Usage of External Key Management Systems	Strict access control are implemented to ensure that only authorised users and systems can access the keys (cf. IAM-01);	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		IAC-20

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
CRY-18.01B.4	Usage of External Key Management Systems	Procedures for the regular rotation and renewal of keys are defined and implemented to ensure the security of the keys (cf. CRY-07);	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
CRY-18.01B.5	Usage of External Key Management Systems	All accesses and operations on the external KMS are logged and monitored to detect and respond to suspicious activities; and	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5		MON-03
CRY-18.01B.6	Usage of External Key Management Systems	The cloud service provider ensures that the external KMS is regularly checked for vulnerabilities (cf. OPS-25) and updated (cf. OPS-28) to meet current threats and technological developments.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	3		VPM-05
CRY-18.01B.6	Usage of External Key Management Systems	The cloud service provider ensures that the external KMS is regularly checked for vulnerabilities (cf. OPS-25) and updated (cf. OPS-28) to meet current threats and technological developments.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
CRY-19.01B	Secure Handling of Customer Managed Keys	The cloud service provider implements procedures and technical safeguards to ensure the secure handling of cryptographic keys managed by cloud service customers. In these procedures, the following aspects are considered:	Functional	Intersects With	Third-Party Cryptographic Keys	CRY-10.6	Mechanisms exist to ensure customers are provided with appropriate key management guidance whenever cryptographic keys are shared.	5		CRY-09.6
CRY-19.01B.1	Secure Handling of Customer Managed Keys	Secure integration of customer-generated keys ('Bring-Your-Own-Key'; BYOK) into the cloud environment;	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-10.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	3		CRY-09.4
CRY-19.01B.1	Secure Handling of Customer Managed Keys	Secure integration of customer-generated keys ('Bring-Your-Own-Key'; BYOK) into the cloud environment;	Functional	Intersects With	Third-Party Cryptographic Keys	CRY-10.6	Mechanisms exist to ensure customers are provided with appropriate key management guidance whenever cryptographic keys are shared.	5		CRY-09.6
CRY-19.01B.2	Secure Handling of Customer Managed Keys	Logging of all activities related to customer-managed keys; and	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5		MON-03
CRY-19.01B.3	Secure Handling of Customer Managed Keys	Definition of access control mechanisms to enable that only authorised users can gain access to customer-managed keys.	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		IAC-20
5.9	Communication Security (COS)	Objective: Ensure the protection of information in networks and the corresponding information processing systems.	Functional	No Relationship	N/A	N/A	N/A	0		
COS-01.01B	Technical Safeguards	Based on the results of a risk assessment carried out according to OIS-07, the cloud service provider has implemented technical safeguards which are suitable to timely detect and respond to attacks on the network of system components used for provisioning of the cloud service.	Functional	Intersects With	Network Intrusion Detection & Prevention Systems (NIDS & NIPS) Monitoring	MON-23	Mechanisms exist to monitor Network Intrusion Detection / Prevention Systems (NIDS / NIPS) technologies on critical systems, key network segments and network choke points.	5		MON-01.1
COS-01.01B	Technical Safeguards	Based on the results of a risk assessment carried out according to OIS-07, the cloud service provider has implemented technical safeguards which are suitable to timely detect and respond to attacks on the network of system components used for provisioning of the cloud service.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-31	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5		NET-08
COS-01.02B	Technical Safeguards	For these technical safeguards, preventive and protective measures are implemented at multiple tiers (defence in depth) within the cloud service to mitigate the risk of breaching the deployed defensive system. This includes network-based cyber attacks such as:	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-06	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5		SEA-03
COS-01.02B.1	Technical Safeguards	Attacks on the basis of irregular incoming or outgoing traffic patterns;	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5		MON-01.3
COS-01.02B.2	Technical Safeguards	Distributed Denial-of-Service (DDoS) attacks;	Functional	Intersects With	Denial of Service (DoS) Protection	NET-21	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	8		NET-02.1
COS-01.02B.3	Technical Safeguards	Spoofing attacks;	Functional	Intersects With	Replay-Resistant Authentication	IAC-03.1	Automated mechanisms exist to employ replay-resistant authentication.	3		IAC-02.2
COS-01.02B.3	Technical Safeguards	Spoofing attacks;	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-31	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	3		NET-08
COS-01.02B.4	Technical Safeguards	Code injection attacks;	Functional	Intersects With	Web Application Firewall (WAF)	NET-34	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	5		WEB-03
COS-01.02B.4	Technical Safeguards	Code injection attacks;	Functional	Intersects With	Malformed Input Testing	TDA-17.3	Mechanisms exist to utilize testing methods to ensure Technology Assets, Applications and/or Services (TAAS) continue to operate as intended when subject to invalid or unexpected inputs on its	3		TDA-09.4
COS-01.02B.5	Technical Safeguards	DNS tunneling; and	Functional	Intersects With	DNS & Content Filtering	NET-17	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5		NET-18
COS-01.02B.6	Technical Safeguards	IoT attacks targeting devices within a network.	Functional	Intersects With	Embedded Technology Security Program	EMB-02	Mechanisms exist to facilitate the implementation of embedded technology controls.	3		EMB-01
COS-01.02B.6	Technical Safeguards	IoT attacks targeting devices within a network.	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-31	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	3		NET-08
COS-01.03B	Technical Safeguards	Data from corresponding technical safeguards implemented (cloud service provider data) is fed into the organisation's SIEM system (cf. OPS-13), so that (counter-) measures regarding correlating events can be initiated. The safeguards are documented, communicated and provided in accordance with SP-01.	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	5		MON-02
COS-01.01AC	Technical Safeguards	Technical safeguards ensure that no unknown (physical or virtual) devices join the cloud service provider's (physical or virtual) network.	Functional	Intersects With	Network Access Control (NAC)	NET-16	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	8		AST-02.5
COS-02.01B	Security Requirements for Connections in the Cloud Service Provider's Network	Specific security requirements are designed, documented and provided for establishing connections within the cloud service provider's network. The security requirements define for the cloud service provider's area of responsibility:	Functional	Intersects With	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5		NET-01
COS-02.01B	Security Requirements for Connections in the Cloud Service Provider's Network	Specific security requirements are designed, documented and provided for establishing connections within the cloud service provider's network. The security requirements define for the cloud service provider's area of responsibility:	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-06	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	3		NET-02
COS-02.01B.1	Security Requirements for Connections in the Cloud Service Provider's Network	In which cases the security zones are to be separated and in which cases cloud service customers are to be logically or physically separated;	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	3		CLD-06
COS-02.01B.1	Security Requirements for Connections in the Cloud Service Provider's Network	In which cases the security zones are to be separated and in which cases cloud service customers are to be logically or physically separated;	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
COS-02.01B.2	Security Requirements for Connections in the Cloud Service Provider's Network	Which communication relationships and which network and application protocols are permitted in each case;	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or	3		CFG-03
COS-02.01B.2	Security Requirements for Connections in the Cloud Service Provider's Network	Which communication relationships and which network and application protocols are permitted in each case;	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5		NET-04
COS-02.01B.3	Security Requirements for Connections in the Cloud Service Provider's Network	How the data traffic for administration and monitoring is separated from each on network level;	Functional	Intersects With	Network Device Plane Segmentation	NET-09	Automated mechanisms exist to separate network appliance functions (e.g., management, control and data planes) to prevent ordinary traffic from accessing functions that: (1) Manage network appliances; and/or (2) Affect network operations.	5		NET-06.8
COS-02.01B.4	Security Requirements for Connections in the Cloud Service Provider's Network	How office networks are secured with firewalls and secure WIFI configurations as well as VPN for remote access;	Functional	Intersects With	Wireless Access Authentication & Encryption	CFG-04.8	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	3		CRY-07
COS-02.01B.4	Security Requirements for Connections in the Cloud Service Provider's Network	How office networks are secured with firewalls and secure WIFI configurations as well as VPN for remote access;	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5		NET-03
COS-02.01B.4	Security Requirements for Connections in the Cloud Service Provider's Network	How office networks are secured with firewalls and secure WIFI configurations as well as VPN for remote access;	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3		NET-14
COS-02.01B.5	Security Requirements for Connections in the Cloud Service Provider's Network	Which internal, cross-partition communication is permitted; and	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	3		NET-04
COS-02.01B.6	Security Requirements for Connections in the Cloud Service Provider's Network	Which cross-network communication is allowed.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	3		NET-04
COS-02.01B.6	Security Requirements for Connections in the Cloud Service Provider's Network	Which cross-network communication is allowed.	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	3		NET-05
COS-03.01B	Monitoring of Connections in the Cloud Service Provider's Network	The cloud service provider distinguishes between trusted and untrusted networks. Based on a risk assessment according to OIS-07, these are separated into different security zones for internal and external network areas (and DMZ, if applicable).	Functional	Intersects With	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	3		NET-03.1
COS-03.01B	Monitoring of Connections in the Cloud Service Provider's Network	The cloud service provider distinguishes between trusted and untrusted networks. Based on a risk assessment according to OIS-07, these are separated into different security zones for internal and external network areas (and DMZ, if applicable).	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06
COS-03.01B	Monitoring of Connections in the Cloud Service Provider's Network	The cloud service provider distinguishes between trusted and untrusted networks. Based on a risk assessment according to OIS-07, these are separated into different security zones for internal and external network areas (and DMZ, if applicable).	Functional	Intersects With	Demilitarized Zones (DMZ)	NET-33	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	5		WEB-02
COS-03.02B	Monitoring of Connections in the Cloud Service Provider's Network	Physical and virtualised network environments are designed and configured to restrict and monitor the established connection to trusted or untrusted networks according to the defined security requirements (cf. COS-02).	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	3		MON-01.3
COS-03.02B	Monitoring of Connections in the Cloud Service Provider's Network	Physical and virtualised network environments are designed and configured to restrict and monitor the established connection to trusted or untrusted networks according to the defined security requirements (cf. COS-02).	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5		NET-03
COS-03.03B	Monitoring of Connections in the Cloud Service Provider's Network	The cloud service provider ensures that the configuration of networks matches the security requirements (cf. COS-02). The cloud service provider reviews at least annually and in case of significant changes to the cloud service the design and implementation of the configuration of the connections with regard to the defined security requirements.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5		CPL-03.2
COS-03.03B	Monitoring of Connections in the Cloud Service Provider's Network	The cloud service provider ensures that the configuration of networks matches the security requirements (cf. COS-02). The cloud service provider reviews at least annually and in case of significant changes to the cloud service the design and implementation of the configuration of the connections with regard to the defined security requirements.	Functional	Intersects With	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	3		NET-01
COS-03.04B	Monitoring of Connections in the Cloud Service Provider's Network	Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-07) and follow-up measures are defined and tracked (cf. OPS-18).	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
COS-03.04B	Monitoring of Connections in the Cloud Service Provider's Network	Identified vulnerabilities and deviations are subject to risk assessment in accordance with the risk management procedure (cf. OIS-07) and follow-up measures are defined and tracked (cf. OPS-18).	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	3		VPM-02
COS-03.05B	Monitoring of Connections in the Cloud Service Provider's Network	At specified intervals, the business justification for using all services, protocols, and ports is reviewed. The review also includes the justifications for compensatory measures for the use of protocols that are considered insecure.	Functional	Intersects With	Periodic Configuration Reviews	CFG-08	Mechanisms exist to periodically review Technology Assets, Applications and/or Services (TAAS) configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5		CFG-03.1
COS-03.05B	Monitoring of Connections in the Cloud Service Provider's Network	At specified intervals, the business justification for using all services, protocols, and ports is reviewed. The review also includes the justifications for compensatory measures for the use of protocols that are considered insecure.	Functional	Intersects With	Identification & Justification of Ports, Protocols & Services	TDA-08.4	Mechanisms exist to require developers and/or process owners to identify, document and justify the business need for the ports, protocols and other services necessary to operate their technology solutions.	5		TDA-02.5
COS-04.01B	Cross-Network Access	Each network perimeter is controlled by security gateways.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	8		NET-03
COS-04.02B	Cross-Network Access	The system access authorisation for cross-network access is based on a security assessment based on the requirements of the cloud service customers.	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	5		NET-05
COS-04.01AS	Cross-Network Access	COS-04.01AS, sharpening COS-04.01B Each network perimeter is controlled by redundant and highly available security gateways.	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5		NET-03
COS-05.01B	Networks for Administration	There are separate networks for the administrative management of the infrastructure and for the operation of management consoles. These networks are logically or physically separated from the cloud service customer's network and protected from unauthorised access by multi-factor authentication (cf. IAM-08).	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
COS-05.01B	Networks for Administration	There are separate networks for the administrative management of the infrastructure and for the operation of management consoles. These networks are logically or physically separated from the cloud service customer's network and protected from unauthorised access by multi-factor authentication (cf. IAM-08).	Functional	Intersects With	Segregation From Enterprise Services	NET-08.2	Mechanisms exist to isolate sensitive and/or regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware and patch management) to those isolated network segments.	3		NET-06.4
COS-05.01B	Networks for Administration	There are separate networks for the administrative management of the infrastructure and for the operation of management consoles. These networks are logically or physically separated from the cloud service customer's network and protected from unauthorised access by multi-factor authentication (cf. IAM-08).	Functional	Intersects With	Network Device Plane Segmentation	NET-09	Automated mechanisms exist to separate network appliance functions (e.g., management, control and data planes) to prevent ordinary traffic from accessing functions that: (1) Manage network appliances; and/or (2) Affect network operations.	5		NET-06.8
COS-05.02B	Networks for Administration	Networks used by the cloud service provider to create, migrate or orchestrate compute workloads (e.g. virtual machines, containers, functions) are physically or logically separated from tenant networks.	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	3		CLD-06
COS-05.02B	Networks for Administration	Networks used by the cloud service provider to create, migrate or orchestrate compute workloads (e.g. virtual machines, containers, functions) are physically or logically separated from tenant networks.	Functional	Intersects With	Network Device Plane Segmentation	NET-09	Automated mechanisms exist to separate network appliance functions (e.g., management, control and data planes) to prevent ordinary traffic from accessing functions that: (1) Manage network appliances; and/or (2) Affect network operations.	5		NET-06.8
COS-05.01AC	Networks for Administration	If there is no physical separation between the administration networks and other networks, the administration network traffic uses state of the art encryption (cf. CRY-01).	Functional	Intersects With	Non-Console Administrative Access	CFG-04.7	Cryptographic mechanisms exist to protect the confidentiality and integrity of non-console administrative access.	5		CRY-06
COS-05.01AC	Networks for Administration	If there is no physical separation between the administration networks and other networks, the administration network traffic uses state of the art encryption (cf. CRY-01).	Functional	Intersects With	Network Device Plane Segmentation	NET-09	Automated mechanisms exist to separate network appliance functions (e.g., management, control and data planes) to prevent ordinary traffic from accessing functions that: (1) Manage network appliances; and/or (2) Affect network operations.	3		NET-06.8
COS-06.01B	Separation of Data Traffic in Jointly Used Network Environments	Cloud service customer data traffic in jointly used network environments is separated on network level according to a documented framework to ensure the confidentiality and integrity of the data transmitted.	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5		CLD-06
COS-06.01B	Separation of Data Traffic in Jointly Used Network Environments	Cloud service customer data traffic in jointly used network environments is separated on network level according to a documented framework to ensure the confidentiality and integrity of the data transmitted.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06
COS-06.01AC	Separation of Data Traffic in Jointly Used Network Environments	In the case of IaaS/PaaS, the secure separation is ensured by physically separated networks or by means of state of the art encryption in combination with logical network separation or	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
COS-06.01AC	Separation of Data Traffic in Jointly Used Network Environments	In the case of IaaS/PaaS, the secure separation is ensured by physically separated networks or by means of state of the art encryption in combination with logical network separation or encapsulation.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06
COS-07.01B	Documentation of the Network Topology	The documentation of the logical structure of the network used to provide or operate the cloud service is traceable and up-to-date, in order to avoid administrative errors during live operation and to ensure timely recovery in the event of incidents in accordance with contractual obligations. The documentation shows:	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	8		AST-04
COS-07.01B.1	Documentation of the Network Topology	How the subnets are allocated;	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AST-04
COS-07.01B.2	Documentation of the Network Topology	How the network is zoned and segmented;	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AST-04
COS-07.01B.2	Documentation of the Network Topology	How the network is zoned and segmented;	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	3		NET-06
COS-07.01B.3	Documentation of the Network Topology	How the network connects with third party and public networks; and	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AST-04
COS-07.01B.4	Documentation of the Network Topology	How the data flows between different subnets and system components within the network to support the management, monitoring and analysis of the network.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AST-04
COS-07.01B.4	Documentation of the Network Topology	How the data flows between different subnets and system components within the network to support the management, monitoring and analysis of the network.	Functional	Intersects With	Data Action Mapping	AST-17.2	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive and/or regulated data is stored, transmitted or processed.	3		AST-02.8
COS-07.02B	Documentation of the Network Topology	The partitions, regions, zones or location in which the cloud service customer data is stored are indicated.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	3		AST-04
COS-07.02B	Documentation of the Network Topology	The partitions, regions, zones or location in which the cloud service customer data is stored are indicated.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	5		CLD-09

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
COS-07.03B	Documentation of the Network Topology	The cloud service provider establishes and maintains an accurate representation of the technical and logical structure of the cloud service provider's systems based on the network topology documentation and the asset inventory (cf. AM-02). The documentation includes the system components that provide security functions and the system components that host the corresponding cloud service customer data and cloud service derived data, or provide sensitive functions.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	3		AST-02
COS-07.03B	Documentation of the Network Topology	The cloud service provider establishes and maintains an accurate representation of the technical and logical structure of the cloud service provider's systems based on the network topology documentation and the asset inventory (cf. AM-02). The documentation includes the system components that provide security functions and the system components that host the corresponding cloud service customer data and cloud service derived data, or provide sensitive functions.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AST-04
COS-07.04B	Documentation of the Network Topology	The network topology documentation is reviewed at least once a year. Timely and appropriate remediation measures address any deviations identified during the review.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5		AST-04
COS-08.01B	Policies for Data Transmission	Policies and procedures with technical and organisational safeguards in order to protect the transmission of cloud service customer data, cloud service derived data, cloud service provider data and account data against unauthorised interception, manipulation, copying, modification, redirection, destruction or malware intrusion are documented, communicated and provided according to SP-01. The policies and procedures establish a reference to the asset classification and labelling (cf. AM-09) and cryptographic mechanisms	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
COS-08.01B	Policies for Data Transmission	Policies and procedures with technical and organisational safeguards in order to protect the transmission of cloud service customer data, cloud service derived data, cloud service provider data and account data against unauthorised interception, manipulation, copying, modification, redirection, destruction or malware intrusion are documented, communicated and provided according to SP-01. The policies and procedures establish a reference to the asset classification and labelling (cf. AM-09) and cryptographic mechanisms	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-37	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive and/or regulated data during transmission over open, public networks.	5		NET-12
COS-08.02B	Policies for Data Transmission	Technical safeguards outlined in the documented policies and procedures to protect the transmission of data are implemented and reviewed regularly, as well as in case of significant changes to the cloud service.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	3		CPL-03.2
COS-08.02B	Policies for Data Transmission	Technical safeguards outlined in the documented policies and procedures to protect the transmission of data are implemented and reviewed regularly, as well as in case of significant changes to the cloud service.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-37	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive and/or regulated data during transmission over open, public networks.	5		NET-12
5.10	Portability and Interoperability (PI)	Objective: Enable the ability to access the cloud service via other cloud services or IT systems of the cloud service customers, to obtain the stored data at the end of the contractual relationship and to securely delete it from the cloud service provider.	Functional	No Relationship	N/A	N/A	N/A	0		
PI-01.01B	Safety of Input and Output Interfaces	For inbound and outbound interfaces through which the cloud service can be accessed by other cloud services or IT systems of cloud service customers, the cloud service provider designs, implements and maintains controls regarding the following aspects:	Functional	Intersects With	Data Handling & Portability	CLD-08	Mechanisms exist to ensure cloud providers use secure protocols for the import, export and management of data in cloud-based Technology Assets, Applications and/or Services (TAAS).	5		CLD-07
PI-01.01B	Safety of Input and Output Interfaces	For inbound and outbound interfaces through which the cloud service can be accessed by other cloud services or IT systems of cloud service customers, the cloud service provider designs, implements and maintains controls regarding the following aspects:	Functional	Intersects With	Application Programming Interface (API) Security	NET-35	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	5		CLD-04
PI-01.01B.1	Safety of Input and Output Interfaces	The use of standardised communication protocols for interactions between different application interfaces to ensure the confidentiality and integrity of the transmitted information according to its protection needs, and the adequate authentication of the user;	Functional	Intersects With	Data Handling & Portability	CLD-08	Mechanisms exist to ensure cloud providers use secure protocols for the import, export and management of data in cloud-based Technology Assets, Applications and/or Services (TAAS).	5		CLD-07
PI-01.01B.1	Safety of Input and Output Interfaces	The use of standardised communication protocols for interactions between different application interfaces to ensure the confidentiality and integrity of the transmitted information according to its protection needs, and the adequate authentication of the user;	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	3		CRY-03
PI-01.01B.2	Safety of Input and Output Interfaces	The use of encryption according to CRY-02 in case of communication over untrusted networks;	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
PI-01.01B.3	Safety of Input and Output Interfaces	The use of standardised data formats and common data processing standards to facilitate information processing interoperability;	Functional	Intersects With	Standardized Virtualization Formats	CLD-09	Mechanisms exist to ensure interoperability by requiring cloud providers to use industry-recognized formats and provide documentation of custom changes for review.	5		CLD-08
PI-01.01B.4	Safety of Input and Output Interfaces	The implementation of mechanisms to validate data integrity and establish backup and recovery processes to ensure data security and reliability during exchange, usage and transfer; and	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
PI-01.01B.4	Safety of Input and Output Interfaces	The implementation of mechanisms to validate data integrity and establish backup and recovery processes to ensure data security and reliability during exchange, usage and transfer; and	Functional	Intersects With	Integrity of Data In Transit	CRY-06	Cryptographic mechanisms exist to detect unauthorized changes to data in transit.	3		CRY-04
PI-01.01B.5	Safety of Input and Output Interfaces	The provision of up-to-date information about the available communication protocols, as well as applicable data formats and data processing standards.	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04
PI-01.02B	Safety of Input and Output Interfaces	The cloud service provider provides suitable technical means for extracting cloud service customer data in accordance with the aforementioned policies and procedures to the cloud service customer. Where data volume, format, or architecture make a customer-driven extraction infeasible, the cloud service provider provides appropriate extraction services to the cloud service customer.	Functional	Intersects With	Data Handling & Portability	CLD-08	Mechanisms exist to ensure cloud providers use secure protocols for the import, export and management of data in cloud-based Technology Assets, Applications and/or Services (TAAS).	5		CLD-07
PI-01.02B	Safety of Input and Output Interfaces	The cloud service provider provides suitable technical means for extracting cloud service customer data in accordance with the aforementioned policies and procedures to the cloud service customer. Where data volume, format, or architecture make a customer-driven extraction infeasible, the cloud service provider provides appropriate extraction services to the cloud service customer.	Functional	Intersects With	Data Portability	PRI-41	Mechanisms exist to format exports of Personal Data (PD) in a structured, machine-readable format that allows data subjects to transfer their PD to another controller without hindrance.	3		PRI-06.6
PI-01.01AC	Safety of Input and Output Interfaces	The cloud service provider sets up an application firewall to protect the administration interfaces for cloud service customers that are accessible over public networks.	Functional	Intersects With	Web Application Firewall (WAF)	NET-34	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	8		WEB-03
PI-01.02AC	Safety of Input and Output Interfaces	The cloud service provides cloud service customers with interfaces for custom identity providers to manage the authentication information of users under the responsibility of the cloud service customer. These interfaces are accompanied by a standardised protocol to facilitate communication between the cloud service and the external identity provider.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	3		IAC-01

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
PI-01.03AC	Safety of Input and Output Interfaces	The interfaces are clearly documented to enable subject matter experts of the cloud service customer to integrate their identity provider with the cloud service.	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04
PI-02.01B	Contractual Agreements for the Provision of Data	In contractual agreements, the following aspects are defined for provisioning of cloud service customer data following termination of the contractual relationship, insofar as these are applicable to the cloud service:	Functional	Intersects With	Data Handling & Portability	CLD-08	Mechanisms exist to ensure cloud providers use secure protocols for the import, export and management of data in cloud-based Technology Assets, Applications and/or Services (TAAS).	3		CLD-07
PI-02.01B	Contractual Agreements for the Provision of Data	In contractual agreements, the following aspects are defined for provisioning of cloud service customer data following termination of the contractual relationship, insofar as these are applicable to the cloud service:	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
PI-02.01B.1	Contractual Agreements for the Provision of Data	Type, scope and format of the cloud service customer data the cloud service provider provides to the cloud service customer;	Functional	Intersects With	Data Handling & Portability	CLD-08	Mechanisms exist to ensure cloud providers use secure protocols for the import, export and management of data in cloud-based Technology Assets, Applications and/or Services (TAAS).	3		CLD-07
PI-02.01B.2	Contractual Agreements for the Provision of Data	Methods for delivering the data to the cloud service customer;	Functional	Intersects With	Data Handling & Portability	CLD-08	Mechanisms exist to ensure cloud providers use secure protocols for the import, export and management of data in cloud-based Technology Assets, Applications and/or Services (TAAS).	3		CLD-07
PI-02.01B.3	Contractual Agreements for the Provision of Data	Conditions and time frames for cloud service customer data provisioning throughout the duration of the contractual relationship;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
PI-02.01B.4	Contractual Agreements for the Provision of Data	Right of termination of the contract and definition of the time frame within which the cloud service provider makes the cloud service customer data available to the cloud service customer after termination of the contract;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
PI-02.01B.5	Contractual Agreements for the Provision of Data	Definition of the point in time as of which the cloud service provider makes the cloud service customer data inaccessible to the cloud service customer and deletes these after termination of the contract;	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	3		DCH-21
PI-02.01B.6	Contractual Agreements for the Provision of Data	The cloud service customers' responsibilities and obligations to cooperate for the provision of the cloud service customer data; and	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-11	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	3		TPM-05.4
PI-02.01B.7	Contractual Agreements for the Provision of Data	Cloud service customer data remains the property of the cloud service customer throughout the entire contractual relationship. After its termination, the data is once again the sole property and possession of the cloud service customer.	Functional	Intersects With	Data Stewardship	DCH-06	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	3		DCH-01.1
PI-02.01B.8	Contractual Agreements for the Provision of Data	The definitions are based on the needs of subject matter experts of potential customers who assess the suitability of the cloud service with regard to a dependency on the cloud service provider as well as legal and regulatory requirements.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
PI-02.01AC	Contractual Agreements for the Provision of Data	The design of the aspects is based on legal and regulatory requirements in the environment of the cloud service provider. The cloud service provider identifies the requirements regularly, at least once a year, and checks these for actuality and adjusts the contractual agreements accordingly.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5		CPL-01
PI-02.01AC	Contractual Agreements for the Provision of Data	The design of the aspects is based on legal and regulatory requirements in the environment of the cloud service provider. The cloud service provider identifies the requirements regularly, at least once a year, and checks these for actuality and adjusts the contractual agreements accordingly.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
PI-02.02AC	Contractual Agreements for the Provision of Data	The cloud service provider also provides cloud service derived data to the cloud service customer upon termination of the contractual relationship. The provision of this data is also defined in the contractual agreements and includes the aspects specified in the basic criterion.	Functional	Intersects With	Data Handling & Portability	CLD-08	Mechanisms exist to ensure cloud providers use secure protocols for the import, export and management of data in cloud-based Technology Assets, Applications and/or Services (TAAS).	3		CLD-07
PI-02.02AC	Contractual Agreements for the Provision of Data	The cloud service provider also provides cloud service derived data to the cloud service customer upon termination of the contractual relationship. The provision of this data is also defined in the contractual agreements and includes the aspects specified in the basic criterion.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
PI-03.01B	Secure Deletion of Data	The cloud service provider's procedures for deleting cloud service customer data, cloud service derived data and account data upon termination of the contractual relationship ensure compliance with the contractual agreements (cf. PI-02). Exceptions are only made if they are required by a valid court order or needed for the fulfilment of known future financial and legal obligations.	Functional	Intersects With	Digital & Non-Digital Media Disposal	DCH-17	Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures.	5		DCH-21
PI-03.01B	Secure Deletion of Data	The cloud service provider's procedures for deleting cloud service customer data, cloud service derived data and account data upon termination of the contractual relationship ensure compliance with the contractual agreements (cf. PI-02). Exceptions are only made if they are required by a valid court order or needed for the fulfilment of known future financial and legal obligations.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	3		DCH-09
PI-03.02B	Secure Deletion of Data	The deletion procedures prevent recovery by forensic means that comply with the established rules of technology.	Functional	Intersects With	Digital Media Sanitization	DCH-18	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	8		DCH-09
PI-03.03B	Secure Deletion of Data	The deletion of the cloud service customer data, cloud service derived data and account data is documented in a manner that enables the cloud service customer to obtain proof of the deletion of its data.	Functional	Intersects With	Digital Media Sanitization Documentation	DCH-18.2	Mechanisms exist to supervise, track, document and verify digital media sanitization and disposal actions.	5		DCH-09.1
5.11	Procurement, Development and Modification of Information Systems (DEV)	Objective: Ensure information security in the development cycle of cloud service system components.	Functional	No Relationship	N/A	N/A	N/A	0		
DEV-01.01B	Policies for the Development/Procurement of System Components	Policies and procedures with technical and organisational measures for the secure development of system components of the cloud service are documented, communicated and provided in accordance with SP-01. The policies and procedures contain guidelines for the entire life cycle of the cloud service and are based on recognised standards and methods with regard to the following aspects:	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5		PRM-07
DEV-01.01B	Policies for the Development/Procurement of System Components	Policies and procedures with technical and organisational measures for the secure development of system components of the cloud service are documented, communicated and provided in accordance with SP-01. The policies and procedures contain guidelines for the entire life cycle of the cloud service and are based on recognised standards and methods with regard to the following aspects:	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06
DEV-01.01B.1	Policies for the Development/Procurement of System Components	Security and quality in software development (requirements, design, implementation, testing and verification), including the existence of a security by design principle, enforcing the consideration of information security requirements in the software development phase;	Functional	Intersects With	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5		SEA-01

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
DEV-01.01B.1	Policies for the Development/Procurement of System Components	Security and quality in software development (requirements, design, implementation, testing and verification), including the existence of a security by design principle, enforcing the consideration of information security requirements in the software development phase;	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06
DEV-01.01B.2	Policies for the Development/Procurement of System Components	Security and quality in software deployment (including continuous delivery);	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	3		CHG-01
DEV-01.01B.2	Policies for the Development/Procurement of System Components	Security and quality in software deployment (including continuous delivery);	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3		TDA-06
DEV-01.01B.3	Policies for the Development/Procurement of System Components	Security and quality in operation (reaction to identified faults and vulnerabilities); and	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3		TDA-06
DEV-01.01B.3	Policies for the Development/Procurement of System Components	Security and quality in operation (reaction to identified faults and vulnerabilities); and	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	3		VPM-02
DEV-01.01B.4	Policies for the Development/Procurement of System Components	Secure coding standards and practices (reduction of vulnerabilities being introduced to the code).	Functional	Intersects With	Software Assurance Maturity Model (SAMM)	TDA-03.1	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	8		TDA-06.3
DEV-01.02B	Policies for the Development/Procurement of System Components	Guidelines for the secure development of the cloud service define principles to ensure the system architecture and software operated by the cloud service provider within the production environment are designed in such a way that access to cloud service customer data by the cloud service provider is minimised wherever possible.	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	3		IAC-21
DEV-01.02B	Policies for the Development/Procurement of System Components	Guidelines for the secure development of the cloud service define principles to ensure the system architecture and software operated by the cloud service provider within the production environment are designed in such a way that access to cloud service customer data by the cloud service provider is minimised wherever possible.	Functional	Intersects With	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	3		SEA-01
DEV-01.03B	Policies for the Development/Procurement of System Components	The cloud service provider defines measures to enforce the specified standards and guidelines as part of the policies and procedures for the secure development of system components of the cloud service.	Functional	Intersects With	Conformity Monitoring	CPL-05	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	3		CPL-03
DEV-01.03B	Policies for the Development/Procurement of System Components	The cloud service provider defines measures to enforce the specified standards and guidelines as part of the policies and procedures for the secure development of system components of the cloud service.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3		TDA-06
DEV-01.01AC	Policies for the Development/Procurement of System Components	In procurement, products are preferred which have been certified according to the 'Common Criteria for Information Technology Security Evaluation' (short: Common Criteria - CC) Evaluation Assurance Level EAL 4. If non-certified products are to be procured instead of available certified products, a risk assessment is carried out in accordance with OIS-07.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
DEV-01.01AC	Policies for the Development/Procurement of System Components	In procurement, products are preferred which have been certified according to the 'Common Criteria for Information Technology Security Evaluation' (short: Common Criteria - CC) Evaluation Assurance Level EAL 4. If non-certified products are to be procured instead of available certified products, a risk assessment is carried out in accordance with OIS-07.	Functional	Intersects With	Product Management	TDA-06	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5		TDA-01.1
DEV-02.01B	Outsourcing of the Development	In the case of outsourced development of the cloud service (or individual system components), specifications regarding the following aspects are contractually agreed between the cloud service provider and the service organisation:	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3		TDA-06
DEV-02.01B	Outsourcing of the Development	In the case of outsourced development of the cloud service (or individual system components), specifications regarding the following aspects are contractually agreed between the cloud service provider and the service organisation:	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
DEV-02.01B.1	Outsourcing of the Development	Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods, ensuring a security level equivalent to that of the cloud service provider's internal development;	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5		TDA-06
DEV-02.01B.1	Outsourcing of the Development	Security in software development (requirements, design, implementation, tests and verifications) in accordance with recognised standards and methods, ensuring a security level equivalent to that of the cloud service provider's internal development;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
DEV-02.01B.2	Outsourcing of the Development	Acceptance testing of the quality of the services provided in accordance with the agreed functional and non-functional requirements; and	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	5		TDA-09
DEV-02.01B.3	Outsourcing of the Development	Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	3		TDA-09
DEV-02.01B.3	Outsourcing of the Development	Providing evidence that sufficient verifications have been carried out to rule out the existence of known vulnerabilities.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	3		VPM-06
DEV-02.02B	Outsourcing of the Development	Before outsourcing the development of the cloud service or components thereof, the cloud service provider conducts a risk assessment according to SSO-02 that takes into account at least the following aspects:	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	3		RSK-09.1
DEV-02.02B	Outsourcing of the Development	Before outsourcing the development of the cloud service or components thereof, the cloud service provider conducts a risk assessment according to SSO-02 that takes into account at least the following aspects:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
DEV-02.02B.1	Outsourcing of the Development	Management of source code by the service organisation;	Functional	Intersects With	Developer Configuration Management	TDA-20	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	5		TDA-14
DEV-02.02B.2	Outsourcing of the Development	Accessability of source code to the cloud service provider;	Functional	Intersects With	Developer Configuration Management	TDA-20	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	5		TDA-14

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
DEV-02.02B.3	Outsourcing of the Development	Human resource procedures implemented by the service organisation;	Functional	Intersects With	Developer Screening	TDA-19	Mechanisms exist to ensure that the developers of Technology Assets, Applications and/or Services (TAAS) have the requisite skillset and appropriate access authorizations.	3		TDA-13
DEV-02.02B.3	Outsourcing of the Development	Human resource procedures implemented by the service organisation;	Functional	Intersects With	Third-Party Personnel Security	TPM-13	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5		TPM-06
DEV-02.02B.4	Outsourcing of the Development	Required access to the development, test and preproduction environments of the cloud service provider; and	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-15.1	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	3		TDA-08
DEV-02.02B.4	Outsourcing of the Development	Required access to the development, test and preproduction environments of the cloud service provider; and	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-04
DEV-02.02B.5	Outsourcing of the Development	Management of subcontractors engaged by the service organisation.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
DEV-02.01AC	Outsourcing of the Development	The cloud service provider documents and implements a procedure that enables the supervision and control of the outsourced development activity to ensure that it complies with the secure development policy of the cloud service provider, and that the security level achieved through it matches the security level achieved through	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3		TDA-06
DEV-02.01AC	Outsourcing of the Development	The cloud service provider documents and implements a procedure that enables the supervision and control of the outsourced development activity to ensure that it complies with the secure development policy of the cloud service provider, and that the security level achieved through it matches the security level achieved through	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
DEV-02.02AC	Outsourcing of the Development	When a change contains work from outsourced development, the cloud service provider's personnel runs the tests needed to decide whether the change can be deployed.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	5		TDA-09
DEV-03.01B	Policies for Changes to System Components	Policies and procedures with procedures and technical safeguards for change management of system components of the cloud service are documented, communicated and provided according to SP-01 with regard to the following aspects:	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	8		CHG-01
DEV-03.01B	Policies for Changes to System Components	Policies and procedures with procedures and technical safeguards for change management of system components of the cloud service are documented, communicated and provided according to SP-01 with regard to the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
DEV-03.01B.1	Policies for Changes to System Components	Criteria for risk assessment, categorisation and prioritisation of changes and related requirements for the type and scope of testing to be performed, and necessary approvals for the development/implementation of the change and releases for deployment in the production environment by authorised personnel or system components;	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	5		CHG-02
DEV-03.01B.1	Policies for Changes to System Components	Criteria for risk assessment, categorisation and prioritisation of changes and related requirements for the type and scope of testing to be performed, and necessary approvals for the development/implementation of the change and releases for deployment in the production environment by authorised personnel or system components;	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5		CHG-03
DEV-03.01B.2	Policies for Changes to System Components	Requirements for the performance and documentation of tests;	Functional	Intersects With	Test, Validate & Document Changes	CHG-07	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented into	5		CHG-02.2
DEV-03.01B.3	Policies for Changes to System Components	Requirements for segregation of duties during development, testing and release of changes;	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5		HRS-11
DEV-03.01B.3	Policies for Changes to System Components	Requirements for segregation of duties during development, testing and release of changes;	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-15.1	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	3		TDA-08
DEV-03.01B.4	Policies for Changes to System Components	Requirements for the proper information of cloud service customers about the type and scope of the change as well as the resulting obligations to cooperate in accordance with the contractual agreements;	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		CHG-05
DEV-03.01B.5	Policies for Changes to System Components	Requirements for the documentation of changes in system, operational and user documentation;	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	3		CHG-02
DEV-03.01B.5	Policies for Changes to System Components	Requirements for the documentation of changes in system, operational and user documentation;	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04
DEV-03.01B.6	Policies for Changes to System Components	Requirements for the implementation and documentation of emergency changes such that - as far as reasonably possible - they comply with the same level of security as normal changes;	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	3		CHG-02
DEV-03.01B.7	Policies for Changes to System Components	Requirements for the handling of unexpected effects of those changes, including corrective actions;	Functional	Intersects With	Control Functionality Verification	CHG-09	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5		CHG-06
DEV-03.01B.8	Policies for Changes to System Components	Requirements for the increased testing for the development of security features that implement technical mechanisms and safeguards; and	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	3		TDA-09
DEV-03.01B.9	Policies for Changes to System Components	Requirements for managing exceptions, including emergency changes, to ensure related risks are appropriately mitigated.	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	3		CHG-02
DEV-03.01B.9	Policies for Changes to System Components	Requirements for managing exceptions, including emergency changes, to ensure related risks are appropriately mitigated.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and	3		GOV-02.1
DEV-04.01B	Safety Training and Awareness Programme Regarding Continuous Software Delivery and Associated Systems,	The cloud service provider provides a training programme for regular, role-based security training and awareness for internal and external personnel on standards and methods for:	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
DEV-04.01B	Safety Training and Awareness Programme Regarding Continuous Software Delivery and Associated Systems,	The cloud service provider provides a training programme for regular, role-based security training and awareness for internal and external personnel on standards and methods for:	Functional	Intersects With	Continuing Professional Education (CPE) - DevOps Personnel	SAT-08	Mechanisms exist to ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure Software Development Practices (SSDP) to appropriately address evolving threats.	5		SAT-03.8
DEV-04.01B.1	Safety Training and Awareness Programme Regarding Continuous Software Delivery and Associated Systems,	Secure software development and provision as well as on how to use the tools used for this purpose; and	Functional	Intersects With	Continuing Professional Education (CPE) - DevOps Personnel	SAT-08	Mechanisms exist to ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure Software Development Practices (SSDP) to appropriately address evolving threats.	5		SAT-03.8
DEV-04.01B.2	Safety Training and Awareness Programme Regarding Continuous Software Delivery and Associated Systems,	Risks linked to malicious code and best practices to reduce the impact of an infection.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		SAT-02
DEV-04.02B	Safety Training and Awareness Programme Regarding Continuous Software Delivery and Associated Systems, Components or Tools	The programme is regularly reviewed and updated with regard to the applicable policies and procedures, the assigned roles and responsibilities and the tools used.	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-03	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	5		SAT-01.1
DEV-05.01B	Design Documentation for Security Features	Design documentation for security features is based on a security analysis of the adequacy and planned effectiveness of the features. A specification of expected inputs, outputs and possible errors is included in the documentation.	Functional	Intersects With	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	3		SEA-01
DEV-05.01B	Design Documentation for Security Features	Design documentation for security features is based on a security analysis of the adequacy and planned effectiveness of the features. A specification of expected inputs, outputs and possible errors is included in the documentation.	Functional	Intersects With	Developer Architecture & Design	TDA-04	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical and logical components; and (3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.	5		TDA-05
DEV-06.01B	Risk Assessment, Categorisation and Prioritisation of Changes	In accordance with the applicable policies, changes are subject to a risk assessment evaluating its potential impact on the overall cloud service in scope. In addition, when multiple changes are implemented concurrently, their mutual interactions and cumulative effects are also subject to the risk assessment in order to identify potential conflicts or dependencies. All identified risks and dependencies are categorised and prioritised accordingly.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	8		CHG-03
DEV-06.02B	Risk Assessment, Categorisation and Prioritisation of Changes	If the risk associated to a planned change is high, appropriate mitigation measures are taken before deploying the change in the cloud service's production environment.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5		CHG-03
DEV-06.02B	Risk Assessment, Categorisation and Prioritisation of Changes	If the risk associated to a planned change is high, appropriate mitigation measures are taken before deploying the change in the cloud service's production environment.	Functional	Intersects With	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	3		RSK-06
DEV-06.01AC	Risk Assessment, Categorisation and Prioritisation of Changes	In accordance with the contractual agreements, meaningful information about the occasion, time, duration, type and scope of the change is submitted to authorised bodies of the cloud service customer so that they can carry out their own risk assessment before the change is made available in the production environment. Regardless of the contractual agreements, this is done for changes that have the highest risk category based on their risk assessment. This does not include changes without an effect on the service usage or security posture of	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		CHG-05
DEV-07.01B	Testing Changes	Changes to the cloud service are subject to appropriate testing according to documented test procedures during software development and deployment.	Functional	Intersects With	Test, Validate & Document Changes	CHG-07	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented into	8		CHG-02.2
DEV-07.01B	Testing Changes	Changes to the cloud service are subject to appropriate testing according to documented test procedures during software development and deployment.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	5		TDA-09
DEV-07.02B	Testing Changes	The type and scope of the tests correspond to the risk assessment. The tests are carried out by appropriately qualified personnel of the cloud service provider or by automated test procedures that comply with established rules of technology. Cloud service customers are involved into the tests in accordance with the contractual requirements.	Functional	Intersects With	Test, Validate & Document Changes	CHG-07	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented into production.	5		CHG-02.2
DEV-07.02B	Testing Changes	The type and scope of the tests correspond to the risk assessment. The tests are carried out by appropriately qualified personnel of the cloud service provider or by automated test procedures that comply with established rules of technology. Cloud service customers are involved into the tests in accordance with the contractual requirements.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	3		TDA-09
DEV-07.03B	Testing Changes	Before using cloud service customer data for tests, the cloud service provider first obtains approval from that cloud service customer and anonymises the cloud service customer data. The cloud service provider ensures the confidentiality of the data during the whole process.	Functional	Intersects With	De-Identification (Anonymization)	DCH-36	Mechanisms exist to de-identify sensitive and/or regulated data through (1) Anonymization; (2) De-identification; (3) Pseudonymization; and/or (4) Redaction.	3		DCH-23
DEV-07.03B	Testing Changes	Before using cloud service customer data for tests, the cloud service provider first obtains approval from that cloud service customer and anonymises the cloud service customer data. The cloud service provider ensures the confidentiality of the data during the whole	Functional	Intersects With	Use of Live Data	TDA-18	Mechanisms exist to approve, document and control the use of live data in development and test environments.	8		TDA-10

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
DEV-07.04B	Testing Changes	The security features of the cloud service are subject to tests that fully cover the security features' specification (cf. DEV-05), including all specified error conditions. The documentation of these tests covers at least the following aspects:	Functional	Intersects With	Developer Architecture & Design	TDA-04	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical and logical components; and (3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.	3		TDA-05
DEV-07.04B	Testing Changes	The security features of the cloud service are subject to tests that fully cover the security features' specification (cf. DEV-05), including all specified error conditions. The documentation of these tests covers at least the following aspects:	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	5		TDA-09
DEV-07.04B.1	Testing Changes	A description of the test;	Functional	Intersects With	Test, Validate & Document Changes	CHG-07	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented into production.	5		CHG-02.2
DEV-07.04B.1	Testing Changes	A description of the test;	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:	3		TDA-09
DEV-07.04B.2	Testing Changes	The initial conditions;	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	3		TDA-09
DEV-07.04B.3	Testing Changes	The expected outcome; and	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	3		TDA-09
DEV-07.04B.4	Testing Changes	Procedures for running the test.	Functional	Intersects With	Test, Validate & Document Changes	CHG-07	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented into production.	5		CHG-02.2
DEV-07.04B.4	Testing Changes	Procedures for running the test.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to:	3		TDA-09
DEV-07.05B	Testing Changes	The severity of the errors and vulnerabilities identified in the tests, which are relevant for the deployment decision, is determined according to defined criteria and actions for timely remediation or mitigation are initiated.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
DEV-07.05B	Testing Changes	The severity of the errors and vulnerabilities identified in the tests, which are relevant for the deployment decision, is determined according to defined criteria and actions for timely remediation or mitigation are initiated.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	3		VPM-02
DEV-07.01AC	Testing Changes	Pre-launch penetration tests are carried out during the test phase of the cloud service in accordance with the penetration test framework (cf. OPS-22 additional criterion). The severity of identified vulnerabilities is assessed according to defined criteria and actions for timely remediation or mitigation are initiated.	Functional	Intersects With	Application Penetration Testing	TDA-17.4	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	8		TDA-09.5
DEV-07.01AC	Testing Changes	Pre-launch penetration tests are carried out during the test phase of the cloud service in accordance with the penetration test framework (cf. OPS-22 additional criterion). The severity of identified vulnerabilities is assessed according to defined criteria and actions for timely remediation or mitigation are initiated.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07
DEV-08.01B	Logging of Changes	System components for version control and software deployment that are used to manage changes to system components of the cloud service in the production environment are subject to a role and rights framework according to IAM-01 and authorisation mechanisms.	Functional	Intersects With	Access Restriction For Change	CHG-04.1	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5		CHG-04
DEV-08.01B	Logging of Changes	System components for version control and software deployment that are used to manage changes to system components of the cloud service in the production environment are subject to a role and rights framework according to IAM-01 and authorisation mechanisms.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	3		IAC-08
DEV-08.02B	Logging of Changes	The configuration of these system components ensures that all changes performed by the cloud service provider to system components in the production environment are recorded and can be traced back to the individuals or system components contributing to their development, deployment or implementation.	Functional	Intersects With	Post Configuration Change Reviews	CHG-11	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	5		CHG-04.1
DEV-08.02B	Logging of Changes	The configuration of these system components ensures that all changes performed by the cloud service provider to system components in the production environment are recorded and can be traced back to the individuals or system components contributing to their development, deployment or implementation.	Functional	Intersects With	Audit Trails	MON-09.1	Mechanisms exist to link system access to individual users or service accounts.	3		MON-03.2
DEV-08.01AC	Logging of Changes	The cloud service provider enforces the role and rights framework by monitoring the changes made to system components of the cloud service in the production environment. Timely and appropriate remediation measures address any deviations identified during monitoring.	Functional	Intersects With	Control Functionality Verification	CHG-09	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	3		CHG-06
DEV-08.01AC	Logging of Changes	The cloud service provider enforces the role and rights framework by monitoring the changes made to system components of the cloud service in the production environment. Timely and appropriate remediation measures address any deviations identified during monitoring.	Functional	Intersects With	Post Configuration Change Reviews	CHG-11	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	5		CHG-04.1
DEV-09.01B	Version Control	The cloud service provider uses a version control system that adequately ensures the confidentiality, integrity and authenticity of the source code during all development stages.	Functional	Intersects With	Software / Firmware Integrity Verification	TDA-20.3	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	5		TDA-14.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
DEV-09.02B	Version Control	Version control procedures track dependencies of individual changes and attribute each change to individual contributors. The version control procedures are capable of restoring affected system components back to a previous state.	Functional	Intersects With	Retention Of Previous Configurations	CFG-09	Mechanisms exist to retain previous versions of secure baseline configuration to support roll back.	3		CFG-02.3
DEV-09.02B	Version Control	Version control procedures track dependencies of individual changes and attribute each change to individual contributors. The version control procedures are capable of restoring affected system components back to a previous state.	Functional	Intersects With	Software / Firmware Integrity Verification	TDA-20.3	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	5		TDA-14.1
DEV-09.03B	Version Control	Version control covers all internally and externally developed software, configurations and third party commercial products under the responsibility of the cloud service provider.	Functional	Intersects With	Software / Firmware Integrity Verification	TDA-20.3	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	3		TDA-14.1
DEV-09.01AC	Version Control	Version control procedures provide appropriate safeguards to ensure that the integrity and availability of cloud service customer data is not compromised when system components are restored back to their previous state.	Functional	Intersects With	Retention Of Previous Configurations	CFG-09	Mechanisms exist to retain previous versions of secure baseline configuration to support roll back.	3		CFG-02.3
DEV-09.01AC	Version Control	Version control procedures provide appropriate safeguards to ensure that the integrity and availability of cloud service customer data is not compromised when system components are restored back to their previous state.	Functional	Intersects With	Software / Firmware Integrity Verification	TDA-20.3	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	3		TDA-14.1
DEV-09.02AC	Version Control	The cloud service provider keeps a record of all deployed software versions and system configurations. This record enables the recreation of a previously implemented environment in a test environment. The retention time for this history is risk-based (cf. OIS-07), defined in the policy for version control and aligned to the support life cycle of the cloud service.	Functional	Intersects With	Retention Of Previous Configurations	CFG-09	Mechanisms exist to retain previous versions of secure baseline configuration to support roll back.	5		CFG-02.3
DEV-10.01B	Approvals for Provision in the Production Environment	Authorised personnel or system components of the cloud service provider approve changes to the cloud service based on defined criteria (e.g. test results and required approvals) before these are made available to the cloud service customers in the production	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	5		CHG-02
DEV-10.01B	Approvals for Provision in the Production Environment	Authorised personnel or system components of the cloud service provider approve changes to the cloud service based on defined criteria (e.g. test results and required approvals) before these are made available to the cloud service customers in the production	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-11.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each Technology Asset, Application and/or Service (TAAS) under their control.	3		GOV-15.4
DEV-10.02B	Approvals for Provision in the Production	Cloud service customers are involved in the release according to contractual agreements.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	3		CHG-05
DEV-10.01AC	Approvals for Provision in the Production Environment	The approval process is monitored. Timely and appropriate remediation measures address any deviations identified during monitoring.	Functional	Intersects With	Control Functionality Verification	CHG-09	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	3		CHG-06
DEV-10.01AC	Approvals for Provision in the Production Environment	The approval process is monitored. Timely and appropriate remediation measures address any deviations identified during monitoring.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
DEV-11.01B	Protection of Development and Test Environments	Development and test environments under the responsibility of the cloud service provider undergo a risk assesssment (cf. OIS-07) and are protected with appropriate security measures against identified risks. This also includes extending the backup plan (cf. OPS-06) to the necessary parts of those environments.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-11
DEV-11.01B	Protection of Development and Test Environments	Development and test environments under the responsibility of the cloud service provider undergo a risk assesssment (cf. OIS-07) and are protected with appropriate security measures against identified risks. This also includes extending the backup plan (cf. OPS-06) to the necessary parts of those environments.	Functional	Intersects With	Secure Development Environments	TDA-15	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	8		TDA-07
DEV-12.01B	Separation of Environments	Production environments are physically or logically separated from test or development environments to prevent unauthorised access to cloud service customer data, the spread of malware, or unintended changes to system components. Cloud service customer data contained in the production environments is not used in test or development environments, unless explicitly approved by cloud service customers, in order not to compromise their confidentiality.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-15.1	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	8		TDA-08
DEV-12.01B	Separation of Environments	Production environments are physically or logically separated from test or development environments to prevent unauthorised access to cloud service customer data, the spread of malware, or unintended changes to system components. Cloud service customer data contained in the production environments is not used in test or development environments, unless explicitly approved by cloud service customers, in order not to compromise their confidentiality.	Functional	Intersects With	Use of Live Data	TDA-18	Mechanisms exist to approve, document and control the use of live data in development and test environments.	3		TDA-10
DEV-12.02B	Separation of Environments	Unless unavoidable, the cloud service provider does not reuse the cryptographic secret and private keys and other secrets used in production environments in other, non-production environments. Any unavoidable reuse of the cryptographic secret and private keys between production and non-production environments is documented and justified in accordance with the process for handling exceptions (cf. SP-03) and the risk management procedures (cf. OIS-07).	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
DEV-13.01B	Transparency about Software Components	The cloud service provider ensures that, as part of the software development process, a list of software components is created, maintained, and kept up-to-date for every developed or integrated software component.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	8		TDA-04.2
DEV-13.02B	Transparency about Software Components	The cloud service provider maintains a list of software components for integrated software components as well, except where such information is not available and cannot be produced with reasonable effort. The risk from these exceptions is treated according to SP-03.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	3		GOV-02.1
DEV-13.02B	Transparency about Software Components	The cloud service provider maintains a list of software components for integrated software components as well, except where such information is not available and cannot be produced with reasonable effort. The risk from these exceptions is treated according to SP-03.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5		TDA-04.2
DEV-14.01B	Secure Use of Third Party Hardware and Software	Policies and procedures for the use of third party and open source software are documented, communicated and provided in accordance with SP-01.	Functional	Intersects With	Open Source Software	CFG-13	Mechanisms exist to establish parameters for the secure use of open source software.	5		CFG-04.1
DEV-14.01B	Secure Use of Third Party Hardware and Software	Policies and procedures for the use of third party and open source software are documented, communicated and provided in accordance with SP-01.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
DEV-14.02B	Secure Use of Third Party Hardware and Software	For the hardware and software products (cf. DEV-13) used in the development of the cloud service, a list of dependencies to those products is maintained.	Functional	Intersects With	Hardware Bill of Materials (HBOM)	TDA-21.2	Mechanisms exist to generate, or obtain, a Hardware Bill of Materials (HBOM) for Technology Assets, Applications and/or Services (TAAS) that lists hardware components in use, including component identifiers, versions and suppliers.	5		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
DEV-14.02B	Secure Use of Third Party Hardware and Software	For the hardware and software products (cf. DEV-13) used in the development of the cloud service, a list of dependencies to those products is maintained.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5		TDA-04.2
DEV-14.03B	Secure Use of Third Party Hardware and Software	Only trusted sources are used to retrieve third party software. Whenever possible, the authenticity of the software is verified.	Functional	Intersects With	Signed Components	CHG-13	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	3		CHG-04.2
DEV-14.03B	Secure Use of Third Party Hardware and Software	Only trusted sources are used to retrieve third party software. Whenever possible, the authenticity of the software is verified.	Functional	Intersects With	Product Tampering and Counterfeiting (PTC)	TDA-09	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5		TDA-11
DEV-14.01AC	Secure Use of Third Party Hardware and Software	In procurement for the development of the cloud service, the cloud service provider performs a risk assessment in accordance with OIS-07 for every hardware and software product.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
DEV-14.01AC	Secure Use of Third Party Hardware and Software	In procurement for the development of the cloud service, the cloud service provider performs a risk assessment in accordance with OIS-07 for every hardware and software product.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
DEV-15.01B	Exceptions to the Change Management Process	The cloud service provider's change management process implements procedures for managing exceptions, including emergency changes, to ensure related risks are appropriately mitigated.	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	5		CHG-01
DEV-15.01B	Exceptions to the Change Management Process	The cloud service provider's change management process implements procedures for managing exceptions, including emergency changes, to ensure related risks are appropriately mitigated.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and	3		GOV-02.1
5.12	Control and Monitoring of Service Providers and	Objective: Ensure the protection of information that service providers or suppliers of the cloud service provider (service organisation) can access and monitor the agreed services and security requirements.	Functional	No Relationship	N/A	N/A	N/A	0		
SSO-01.01B	Policies and Procedures for Controlling and Monitoring Service Organisations	Policies and procedures for controlling and monitoring service organisations whose services contribute to the development or operation of the cloud service are documented, communicated and provided in accordance with SP-01 with respect to the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
SSO-01.01B	Policies and Procedures for Controlling and Monitoring Service Organisations	Policies and procedures for controlling and monitoring service organisations whose services contribute to the development or operation of the cloud service are documented, communicated and provided in accordance with SP-01 with respect to the following aspects:	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	8		TPM-01
SSO-01.01B.1	Policies and Procedures for Controlling and Monitoring Service Organisations	Requirements for the assessment of risks resulting from the procurement of third-party services;	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-20	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	3		RSK-09
SSO-01.01B.1	Policies and Procedures for Controlling and Monitoring Service Organisations	Requirements for the assessment of risks resulting from the procurement of third-party services;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
SSO-01.01B.2	Policies and Procedures for Controlling and Monitoring Service Organisations	Requirements for the classification of service organisations based on the risk assessment by the cloud service provider and the determination of whether the service organisation is a subservice organisation;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5		TPM-02
SSO-01.01B.3	Policies and Procedures for Controlling and Monitoring Service Organisations	Information security requirements for the processing, storage or transmission of information by service organisations based on the established rules of technology, and under consideration of the criteria in this catalogue;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
SSO-01.01B.4	Policies and Procedures for Controlling and Monitoring Service Organisations	Information security awareness and training requirements for personnel;	Functional	Intersects With	Vendor-Specific Security, Compliance & Resilience Training	SAT-05.4	Mechanisms exist to incorporate vendor-specific security, compliance and resilience training in support of new technology initiatives.	5		SAT-03.4
SSO-01.01B.5	Policies and Procedures for Controlling and Monitoring Service Organisations	Applicable legal and regulatory requirements;	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5		CPL-01
SSO-01.01B.6	Policies and Procedures for Controlling and Monitoring Service Organisations	Requirements for dealing with vulnerabilities, security incidents and incidents;	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-21	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5		TPM-11
SSO-01.01B.7	Policies and Procedures for Controlling and Monitoring Service Organisations	Specifications for the contractual agreement of these requirements;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
SSO-01.01B.8	Policies and Procedures for Controlling and Monitoring Service Organisations	Specifications for the monitoring of these requirements; and	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
SSO-01.01B.9	Policies and Procedures for Controlling and Monitoring Service Organisations	Specifications for applying these requirements also to subservice organisations used by the service organisations, insofar as the services provided by these subservice organisations also contribute to the development or operation of the cloud service.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	8		TPM-05.2
SSO-01.01AC	Policies and Procedures for Controlling and Monitoring Service Organisations	Subservice organisations of the cloud service provider are contractually obliged to provide regular reports by independent auditors on the suitability of the design and operating effectiveness of their service-related system of internal control system that allow the cloud service provider to determine whether the subservice organisation designed and operated controls that are commensurate with the expected complementary subservice organisation controls	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	8		TPM-05.8
SSO-01.02AC	Policies and Procedures for Controlling and Monitoring Service Organisations	In case no such reports can be provided, the cloud service provider agrees appropriate information and audit rights to assess the design and operations of the service-related system of internal control regarding the expected CSOC.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	5		TPM-05
SSO-01.02AC	Policies and Procedures for Controlling and Monitoring Service Organisations	In case no such reports can be provided, the cloud service provider agrees appropriate information and audit rights to assess the design and operations of the service-related system of internal control regarding the expected CSOC.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
SSO-02.01B	Risk Assessment of Service Organisations	Service organisations of the cloud service provider undergo a risk assessment in accordance with the policies and procedures for the control and monitoring of service organisations prior to contributing to the development or operation of the cloud service. The risk assessment includes the identification, analysis, evaluation, treatment and documentation of risks with regard to the following aspects:	Functional	Intersects With	Supply Chain Risk Assessment (SCRA)	RSK-21	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5		RSK-09.1
SSO-02.01B	Risk Assessment of Service Organisations	Service organisations of the cloud service provider undergo a risk assessment in accordance with the policies and procedures for the control and monitoring of service organisations prior to contributing to the development or operation of the cloud service. The risk assessment includes the identification, analysis, evaluation, treatment and documentation of risks with regard to the following aspects:	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	8		TPM-04.1
SSO-02.01B.1	Risk Assessment of Service Organisations	Protection needs regarding the confidentiality, integrity, availability and authenticity of cloud service customer data, cloud service derived data, cloud service provider data and account data processed, stored or transmitted by the service organisation;	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	3		DCH-02
SSO-02.01B.1	Risk Assessment of Service Organisations	Protection needs regarding the confidentiality, integrity, availability and authenticity of cloud service customer data, cloud service derived data, cloud service provider data and account data processed, stored or transmitted by the service organisation;	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
SSO-02.01B.2	Risk Assessment of Service Organisations	Impact of a protection breach on the provision of the cloud service;	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	3		RSK-08
SSO-02.01B.2	Risk Assessment of Service Organisations	Impact of a protection breach on the provision of the cloud service;	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
SSO-02.01B.3	Risk Assessment of Service Organisations	The cloud service provider's dependence on the service organisation for the scope, complexity and uniqueness of the provided service, including the consideration of possible alternatives;	Functional	Intersects With	Approved Technologies	AST-10	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	3		AST-01.4
SSO-02.01B.3	Risk Assessment of Service Organisations	The cloud service provider's dependence on the service organisation for the scope, complexity and uniqueness of the provided service, including the consideration of possible alternatives;	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-04	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	3		TPM-03
SSO-02.01B.4	Risk Assessment of Service Organisations	Complementary subservice organisation controls (CSOCs) assumed in the design of cloud service provider's controls to meet the applicable C5 criteria;	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-11	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	3		TPM-05.4
SSO-02.01B.5	Risk Assessment of Service Organisations	Deviations regarding the design and operation of CSOCs assumed at service organisations considered as subservice organisations and mitigating measures by the cloud service provider to address such deviations;	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-18	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5		TPM-09
SSO-02.01B.6	Risk Assessment of Service Organisations	The ability of the cloud service provider to diversify sources of supply and limit vendor lock-in;	Functional	Intersects With	Supplier Diversity	TPM-06	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	5		TDA-03.1
SSO-02.01B.7	Risk Assessment of Service Organisations	Whether service organisations used by the cloud service provider themselves use subcontracted service organisations (subcontractors) that contribute to the development and operation of the cloud service; and	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
SSO-02.01B.8	Risk Assessment of Service Organisations	If service organisations used by the cloud service provider themselves use subcontractors, the types of data processed by the subcontractors.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	3		TPM-04.4
SSO-02.01B.8	Risk Assessment of Service Organisations	If service organisations used by the cloud service provider themselves use subcontractors, the types of data processed by the subcontractors.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	3		TPM-05.2
SSO-02.02B	Risk Assessment of Service Organisations	The adequacy of the risk assessment is reviewed regularly, at least annually, by qualified personnel of the cloud service provider during service usage.	Functional	Intersects With	Risk Assessment Update	RSK-13.2	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	3		RSK-07
SSO-02.02B	Risk Assessment of Service Organisations	The adequacy of the risk assessment is reviewed regularly, at least annually, by qualified personnel of the cloud service provider during service usage.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5		TPM-04.1
SSO-03.01B	Data Processing of Service Organisations	If the cloud service provider relies on assets from a supplier or on services from subservice organisations for the operation of the cloud service, it does not allow those suppliers or service organisations to access any cloud service customer data, cloud service derived data or account data. Exceptions are made only if the cloud service provider has performed a risk assessment according to OIS-07 on the possibility of cloud service customer data, cloud service derived data or account data being exposed.	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	3		IAC-20
SSO-03.01B	Data Processing of Service Organisations	If the cloud service provider relies on assets from a supplier or on services from subservice organisations for the operation of the cloud service, it does not allow those suppliers or service organisations to access any cloud service customer data, cloud service derived data or account data. Exceptions are made only if the cloud service provider has performed a risk assessment according to OIS-07 on the possibility of cloud service customer data, cloud service derived data or account data being exposed.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
SSO-03.02B	Data Processing of Service Organisations	The cloud service provider obtains written authorisation of the customer prior to the processing of cloud service customer data, cloud service derived data or account data when engaging service organisations. This can be achieved by authorisation of the customer, per service organisation, or by way of a general pre-authorisation between the cloud service provider and the customer.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	3		TPM-04.4
SSO-03.02B	Data Processing of Service Organisations	The cloud service provider obtains written authorisation of the customer prior to the processing of cloud service customer data, cloud service derived data or account data when engaging service organisations. This can be achieved by authorisation of the customer, per service organisation, or by way of a general pre-authorisation between the cloud service provider and the customer.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
SSO-03.01AS	Data Processing of Service Organisations	SSO-03.01AS, sharpening SSO-03.01B If the cloud service provider relies on assets from a supplier or on services from subservice organisations for the operation of the cloud service, it does not allow those suppliers or service organisations to access any cloud service customer data, cloud service derived data or account data. Exceptions are made only if the cloud service provider has performed a risk assessment according to OIS-07 on the possibility of cloud service customer data, cloud service derived data or account data being exposed, and it is ensured that all operations requiring access to those data types are performed or supervised by authorised personnel (cf. HR-01).	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	3		IAC-20
SSO-03.01AS	Data Processing of Service Organisations	SSO-03.01AS, sharpening SSO-03.01B If the cloud service provider relies on assets from a supplier or on services from subservice organisations for the operation of the cloud service, it does not allow those suppliers or service organisations to access any cloud service customer data, cloud service derived data or account data. Exceptions are made only if the cloud service provider has performed a risk assessment according to OIS-07 on the possibility of cloud service customer data, cloud service derived data or account data being exposed, and it is ensured that all operations requiring access to those data types are performed or supervised by authorised personnel (cf. HR-01).	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
SSO-04.01B	Directory of Service Organisations	The cloud service provider maintains a directory for controlling and monitoring the service organisations that contribute services to the delivery of the cloud service. The following information is maintained in the directory:	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8		TPM-01.1
SSO-04.01B.1	Directory of Service Organisations	Company name;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-04.01B.2	Directory of Service Organisations	Address of the head office;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-04.01B.3	Directory of Service Organisations	Applicable legal jurisdiction;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-04.01B.4	Directory of Service Organisations	Locations where cloud service customer data, cloud service derived data, cloud service provider data and account data is processed and stored;	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	3		CLD-09
SSO-04.01B.4	Directory of Service Organisations	Locations where cloud service customer data, cloud service derived data, cloud service provider data and account data is processed and stored;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-04.01B.5	Directory of Service Organisations	Responsible contact group/person at the service organisation;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-04.01B.6	Directory of Service Organisations	Responsible contact group/person at the cloud service provider;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-04.01B.7	Directory of Service Organisations	Description of the service;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-04.01B.8	Directory of Service Organisations	Classification based on the risk assessment;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
SSO-04.01B.9	Directory of Service Organisations	Beginning of service usage; and	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-04.01B.10	Directory of Service Organisations	Proof of compliance with contractually agreed requirements.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
SSO-04.02B	Directory of Service Organisations	The inventory is reviewed at least annually for completeness, accuracy and validity of the information.	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
SSO-05.01B	Monitoring of Compliance with Requirements	The cloud service provider monitors compliance with information security requirements and applicable legal and regulatory requirements in accordance with policies and procedures concerning controlling and monitoring of service organisation.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	8		TPM-08
SSO-05.02B	Monitoring of Compliance with Requirements	Monitoring includes a regular review of the following information to the extent that such information is to be provided by service organisations in accordance with the contractual agreements:	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
SSO-05.02B.1	Monitoring of Compliance with Requirements	Reports on the quality of the service provided;	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
SSO-05.02B.2	Monitoring of Compliance with Requirements	Certificates of the management systems' compliance with international standards;	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5		TPM-05.8
SSO-05.02B.3	Monitoring of Compliance with Requirements	Records of the service organisations on the handling of vulnerabilities, security incidents and incidents;	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-21	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5		TPM-11
SSO-05.02B.4	Monitoring of Compliance with Requirements	Independent third party reports on the design and operation of their service-related system of internal control; and	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-23	Mechanisms exist to obtain an attestation from an independent Third-Party Assessment Organization (3PAO) that provides assurance of conformity with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to contractors and subcontractors.	5		TPM-05.8
SSO-05.02B.5	Monitoring of Compliance with Requirements	If service organisations used by the cloud service provider themselves use subcontractors, the compliance of their subcontractors with relevant contractual, legal and regulatory requirements.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	5		TPM-05.2
SSO-05.02B.5	Monitoring of Compliance with Requirements	If service organisations used by the cloud service provider themselves use subcontractors, the compliance of their subcontractors with relevant contractual, legal and regulatory requirements.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
SSO-05.03B	Monitoring of Compliance with Requirements	The frequency of the monitoring corresponds to the classification of the service organisation based on the risk assessment conducted by the cloud service provider (cf. SSO-02).	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
SSO-05.04B	Monitoring of Compliance with Requirements	If a service organisation is considered to be a subservice organisation, the cloud service provider assesses this relationship and carries out appropriate procedures to ensure that the applicable C5 criteria are met. Appropriate procedures provide reasonable assurance:	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
SSO-05.04B.1	Monitoring of Compliance with Requirements	That the subservice organisation has designed and operated relevant controls; and	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
SSO-05.04B.2	Monitoring of Compliance with Requirements	That the subservice organisation's controls correspond to the expected complementary subservice organisation controls (CSOCs) assumed in the design of the cloud service providers controls.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
SSO-05.05B	Monitoring of Compliance with Requirements	Identified deviations are subjected to analysis, evaluation and treatment in accordance with the risk assessment of service organisations (cf. SSO-02).	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-18	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5		TPM-09
SSO-05.06B	Monitoring of Compliance with Requirements	If a service organisation contributing to the provision of the cloud service undergoes a change that has a significant adverse effect on the cloud service provider's level of security, the cloud service provider communicates this to all of its cloud service customers without undue delay.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		CHG-05
SSO-05.06B	Monitoring of Compliance with Requirements	If a service organisation contributing to the provision of the cloud service undergoes a change that has a significant adverse effect on the cloud service provider's level of security, the cloud service provider communicates this to all of its cloud service customers without undue delay.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	3		IRO-10
SSO-05.07B	Monitoring of Compliance with Requirements	The cloud service provider establishes and documents a procedure to regularly review non-disclosure or confidentiality requirements for all service organisations involved in providing the cloud service. This procedure is implemented in practice, and the review is conducted at least once per year.	Functional	Intersects With	Confidentiality Agreements	HRS-07.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties.	5		HRS-06.1
SSO-05.07B	Monitoring of Compliance with Requirements	The cloud service provider establishes and documents a procedure to regularly review non-disclosure or confidentiality requirements for all service organisations involved in providing the cloud service. This procedure is implemented in practice, and the review is conducted at least once per year.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
SSO-05.01AC	Monitoring of Compliance with Requirements	The procedures for monitoring compliance with the requirements are supplemented by automatic procedures relating to the following aspects:	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
SSO-05.01AC.1	Monitoring of Compliance with Requirements	Configuration of system components;	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	3		CFG-06
SSO-05.01AC.2	Monitoring of Compliance with Requirements	Performance and availability of system components;	Functional	Intersects With	Performance Monitoring	CAP-05	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical Technology Assets, Applications and/or Services (TAAS).	3		CAP-04
SSO-05.01AC.3	Monitoring of Compliance with Requirements	Response time to incidents and security incidents; and	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-21	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	3		TPM-11
SSO-05.01AC.4	Monitoring of Compliance with Requirements	Recovery time (time until completion of error handling).	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-01.4
SSO-05.02AC	Monitoring of Compliance with Requirements	Identified violations and discrepancies are automatically reported to the responsible personnel or system components of the cloud service provider for prompt assessment and action.	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	3		MON-01.4
SSO-05.02AC	Monitoring of Compliance with Requirements	Identified violations and discrepancies are automatically reported to the responsible personnel or system components of the cloud service provider for prompt assessment and action.	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-18	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	3		TPM-09
SSO-05.03AC	Monitoring of Compliance with Requirements	The cloud service provider defines and implements a process for conducting periodic security assessments for all service organisations. The nature and scope of these security assessments correspond to the risk associated with each service organisation. These risk-based security assessments ensure that service organisations meet the required security standards and that any potential risks are identified and mitigated appropriately.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
SSO-05.03AC	Monitoring of Compliance with Requirements	The cloud service provider defines and implements a process for conducting periodic security assessments for all service organisations. The nature and scope of these security assessments correspond to the risk associated with each service organisation. These risk-based security assessments ensure that service organisations meet the required security standards and that any potential risks are identified and mitigated appropriately.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
SSO-06.01B	Contract Termination Strategy for Service Organisations	The cloud service provider has defined and documented contract termination or exit strategies for the purchase of services where the risk assessment of the service organisations regarding the scope, complexity and uniqueness of the service provided resulted in a very high dependency (cf. Supplementary Information).	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	8		TPM-05.7
SSO-06.02B	Contract Termination Strategy for Service Organisations	Exit strategies are aligned with operational continuity plans and include the following aspects:	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
SSO-06.02B	Contract Termination Strategy for Service Organisations	Exit strategies are aligned with operational continuity plans and include the following aspects:	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	5		TPM-05.7
SSO-06.02B.1	Contract Termination Strategy for Service Organisations	Analysis of the potential costs, impacts, resources and timing of the transition of a purchased service to an alternative service organisation;	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	3		TPM-05.7
SSO-06.02B.2	Contract Termination Strategy for Service Organisations	Definition and allocation of roles, responsibilities and sufficient resources to perform the activities for a transition;	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	3		TPM-05.7
SSO-06.02B.3	Contract Termination Strategy for Service Organisations	Definition of success criteria for the transition; and	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	3		TPM-05.7
SSO-06.02B.4	Contract Termination Strategy for Service Organisations	Definition of indicators for monitoring the performance of services, which should initiate the withdrawal from the service if the results are unacceptable.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
SSO-06.02B.4	Contract Termination Strategy for Service Organisations	Definition of indicators for monitoring the performance of services, which should initiate the withdrawal from the service if the results are unacceptable.	Functional	Intersects With	Break Clauses	TPM-19	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for security, compliance and/or resilience controls.	3		TPM-05.7

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
SSO-07.01B	Ensuring Transparency within Service Organisations	The cloud service provider designs, implements and maintains controls to ensure transparency within its service organisations with respect to the following aspects:	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
SSO-07.01B.1	Ensuring Transparency within Service Organisations	Data flow and interfaces between the cloud service provider and service organisations used by the cloud service provider are documented, including measures regarding the secure transmission and access control for data shared with service organisations; and	Functional	Intersects With	Data Action Mapping	AST-17.2	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive and/or regulated data is stored, transmitted or processed.	5		AST-02.8
SSO-07.01B.1	Ensuring Transparency within Service Organisations	Data flow and interfaces between the cloud service provider and service organisations used by the cloud service provider are documented, including measures regarding the secure transmission and access control for data shared with service organisations; and	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-37	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive and/or regulated data during transmission over open, public networks.	3		NET-12
SSO-07.01B.2	Ensuring Transparency within Service Organisations	Cloud service customers are informed of service organisations used by the cloud service provider for development and operation of the cloud service and what type of data these service organisations and their subcontractors are processing.	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-07.01B.3	Ensuring Transparency within Service Organisations	Cloud service customers are informed which of the service organisations themselves use subcontractors to process cloud service customer data.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	3		TPM-05.2
SSO-07.02B	Ensuring Transparency within Service Organisations	The cloud service provider documents this information and reviews its completeness, accuracy and validity at least annually.	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-07.01AS	Ensuring Transparency within Service Organisations	SSO-07.01AS, sharpening SSO-07.01B The cloud service provider designs, implements and maintains controls to ensure transparency within its service organisations with respect to the following aspects:	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
SSO-07.01AS.1	Ensuring Transparency within Service Organisations	Data flow and interfaces between the cloud service provider and service organisations used by the cloud service provider are documented, including measures regarding the secure transmission and access control for data shared with service organisations; and	Functional	Intersects With	Data Action Mapping	AST-17.2	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive and/or regulated data is stored, transmitted or processed.	5		AST-02.8
SSO-07.01AS.1	Ensuring Transparency within Service Organisations	Data flow and interfaces between the cloud service provider and service organisations used by the cloud service provider are documented, including measures regarding the secure transmission and access control for data shared with service organisations; and	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-37	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive and/or regulated data during transmission over open, public networks.	3		NET-12
SSO-07.01AS.2	Ensuring Transparency within Service Organisations	Cloud service customers are informed of service organisations and their subcontractors used by the cloud service provider for development and operation of the cloud service and what type of data these service organisations and their subcontractors are processing.	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-01.1
SSO-07.01AS.3	Ensuring Transparency within Service Organisations	Cloud service customers are informed which of the service organisations themselves use subcontractors to process cloud service customer data.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-14.1	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable subcontractors and suppliers.	3		TPM-05.2
SSO-08.01B	Controlling Exchanges with Suppliers of Functional Components	When functional components used for the provision of the cloud service may directly or indirectly access cloud service customer data, the cloud service provider defines and implements a policy according to SP-01 that does not allow a direct exchange between such components and their suppliers.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	3		NET-04
SSO-08.01B	Controlling Exchanges with Suppliers of Functional Components	When functional components used for the provision of the cloud service may directly or indirectly access cloud service customer data, the cloud service provider defines and implements a policy according to SP-01 that does not allow a direct exchange between such components and their suppliers.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-04
SSO-08.02B	Controlling Exchanges with Suppliers of Functional Components	In addition, procedures are defined and implemented according to SP-01 that require the cloud service provider to authorise any content provided by a supplier for its functional components or to be sent from a functional component to its supplier. The authorisation takes place before the content is transferred and for each transfer.	Functional	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	3		DCH-14
SSO-08.02B	Controlling Exchanges with Suppliers of Functional Components	In addition, procedures are defined and implemented according to SP-01 that require the cloud service provider to authorise any content provided by a supplier for its functional components or to be sent from a functional component to its supplier. The authorisation takes place before the content is transferred and for each transfer.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	3		NET-04
SSO-08.03B	Controlling Exchanges with Suppliers of Functional Components	When a procedure for authorising content before its transfer is automated, the cloud service provider implements it using a solution that maintains traces of:	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
SSO-08.03B.1	Controlling Exchanges with Suppliers of Functional Components	The operations that are proposed by the functional component's supplier;	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
SSO-08.03B.2	Controlling Exchanges with Suppliers of Functional Components	The verification that is performed to authorise the content before its transfer; and	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
SSO-08.03B.3	Controlling Exchanges with Suppliers of Functional Components	The transfers, both incoming and outgoing, that are effectively performed.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
5.13	Security Incident Management (SIM)	Objective: Ensure a consistent and comprehensive approach to the capturing, evaluation, communication and handling of security incidents.	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
SIM-01.01B	Policy for Security Incident Management	Policies, procedures and technical safeguards are documented, communicated and provided in accordance with SP-01 to ensure a fast, effective and proper response to all known security incidents. The cloud service provider defines guidelines for the classification, prioritisation, escalation and root cause analysis of security incidents and creates interfaces to the incident management and business continuity management.	Functional	Intersects With	Incident Response Operations	IRO-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	8		IRO-01
SIM-01.01B	Policy for Security Incident Management	Policies, procedures and technical safeguards are documented, communicated and provided in accordance with SP-01 to ensure a fast, effective and proper response to all known security incidents. The cloud service provider defines guidelines for the classification, prioritisation, escalation and root cause analysis of security incidents and creates interfaces to the incident management and business continuity management.	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	3		IRO-02.4
SIM-01.02B	Policy for Security Incident Management	The cloud service provider has set up a 'Computer Security Incident Response Team' (CSIRT), which contributes to the coordinated resolution of occurring security incidents.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	8		IRO-07
SIM-01.03B	Policy for Security Incident Management	Communication channels with the cloud service customers are identified and defined and customers affected by security incidents are informed in a timely and appropriate manner.	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-15	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	3		IRO-14
SIM-01.03B	Policy for Security Incident Management	Communication channels with the cloud service customers are identified and defined and customers affected by security incidents are informed in a timely and appropriate manner.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
SIM-01.04B	Policy for Security Incident Management	There are procedures as to how the data of a suspicious system can be collected in a conclusive manner in the event of a security incident.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5		IRO-08
SIM-02.01B	Security Incident Response Plans	The cloud service provider has documented, approved and communicated one or more security incident response plans. The plans address all stages of incident response, including identification, containment, eradication, recovery, and lessons learned. They are approved by subject matter experts of the cloud service provider and communicated to all relevant stakeholders.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	3		IRO-02
SIM-02.01B	Security Incident Response Plans	The cloud service provider has documented, approved and communicated one or more security incident response plans. The plans address all stages of incident response, including identification, containment, eradication, recovery, and lessons learned. They are approved by subject matter experts of the cloud service provider and communicated to all relevant stakeholders.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8		IRO-04
SIM-02.02B	Security Incident Response Plans	The plans are evaluated and updated at least annually or as necessary to reflect changes in the organisational structure or environment.	Functional	Intersects With	Data Breach	IRO-22	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.	5		IRO-04.1
SIM-03.01B	Processing of Security Incidents	Subject matter experts of the cloud service provider classify, prioritise and perform root-cause analyses for events that could constitute a security incident.	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5		IRO-02.4
SIM-03.01B	Processing of Security Incidents	Subject matter experts of the cloud service provider classify, prioritise and perform root-cause analyses for events that could constitute a security incident.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
SIM-03.02B	Processing of Security Incidents	The results of these root-cause analyses are documented, shared with relevant stakeholders, and used as part of evaluation and learning processes.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5		IRO-13
SIM-03.03B	Processing of Security Incidents	If the cloud service provider determines that it requires external assistance for processing a security incident, it selects an incident response service based on their competence and trustworthiness or by following the recommendations of a national cybersecurity authority.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	3		IRO-07
SIM-03.03B	Processing of Security Incidents	If the cloud service provider determines that it requires external assistance for processing a security incident, it selects an incident response service based on their competence and trustworthiness or by following the recommendations of a national cybersecurity authority.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
SIM-03.04B	Processing of Security Incidents	A catalogue providing clear identification of information security incidents affecting cloud service customer data is maintained and used for the classification of information security incidents.	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5		IRO-02.4
SIM-03.05B	Processing of Security Incidents	The cloud service provider also uses the incident classification mechanism for the correlation of information security events, and assesses as well as classifies the correlated information security events according to their criticality.	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	3		IRO-02.4
SIM-03.05B	Processing of Security Incidents	The cloud service provider also uses the incident classification mechanism for the correlation of information security events, and assesses as well as classifies the correlated information security events according to their criticality.	Functional	Intersects With	Correlate Monitoring Information	MON-08	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5		MON-02.1
SIM-03.06B	Processing of Security Incidents	All documents and evidence that provide details on security incidents related to the cloud service are archived in a secure and tamper-proof manner, in line with criticality and regulatory requirements.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5		IRO-08
SIM-03.06B	Processing of Security Incidents	All documents and evidence that provide details on security incidents related to the cloud service are archived in a secure and tamper-proof manner, in line with criticality and regulatory requirements.	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	3		MON-08
SIM-03.07B	Processing of Security Incidents	The analysis process provides sufficient traceability to understand root causes and attack progression, appropriate to the risk and impact of the security incident.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	3		IRO-08
SIM-03.07B	Processing of Security Incidents	The analysis process provides sufficient traceability to understand root causes and attack progression, appropriate to the risk and impact of the security incident.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5		IRO-13
SIM-03.01AC	Processing of Security Incidents	The cloud service provider simulates the identification, analysis and defence of security incidents and attacks at least once a year through appropriate tests and exercises (e.g. Red Team training).	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06
SIM-03.01AC	Processing of Security Incidents	The cloud service provider simulates the identification, analysis and defence of security incidents and attacks at least once a year through appropriate tests and exercises (e.g. Red Team training).	Functional	Intersects With	Red Team Exercises	VPM-21	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	5		VPM-10
SIM-03.02AC	Processing of Security Incidents	An integrated team of forensic/incident responder personnel, specifically qualified to preserve evidence and manage a chain of custody, is established or contracted for their services.	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	8		IRO-08

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
SIM-03.03AC	Processing of Security Incidents	The cloud service provider verifies the application of incident management policies and procedures by monitoring the information security incident handling processes. Timely and appropriate remediation measures address any deviations identified during monitoring.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
SIM-03.03AC	Processing of Security Incidents	The cloud service provider verifies the application of incident management policies and procedures by monitoring the information security incident handling processes. Timely and appropriate remediation measures address any deviations identified during monitoring.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	3		IRO-02
SIM-04.01B	Documentation and Reporting of Security Incidents	After a security incident has been processed, the solution is documented in accordance with the contractual agreements and the documentation is sent to the affected customers for final acknowledgement or, if applicable, as confirmation.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
SIM-04.02B	Documentation and Reporting of Security Incidents	Information on security incidents or confirmed security breaches is made available to all affected customers.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
SIM-04.01AC	Documentation and Reporting of Security Incidents	The customer can either actively approve solutions or the solution is automatically approved after a certain period.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	3		IRO-10
SIM-04.02AC	Documentation and Reporting of Security Incidents	The contract between the cloud service provider and the cloud service customer regulates which data is made available to the cloud service customer for his own analysis in the event of security incidents.	Functional	Intersects With	Multi-Tenant Forensics Capabilities	CLD-07.2	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate prompt forensic investigations in the event of a suspected or confirmed security incident.	3		CLD-06.3
SIM-04.02AC	Documentation and Reporting of Security Incidents	The contract between the cloud service provider and the cloud service customer regulates which data is made available to the cloud service customer for his own analysis in the event of security incidents.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
SIM-05.01B	Duty of the Personnel to Report Security Incidents to a Central Body	The cloud service provider informs personnel and external business partners of their obligations. If necessary, they agree to or are contractually obliged to timely report all security events that become known to them and are directly related to the cloud service provided by the cloud service provider to a previously designated central office of the cloud service provider.	Functional	Intersects With	Terms of Employment	HRS-06	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	3		HRS-05
SIM-05.01B	Duty of the Personnel to Report Security Incidents to a Central Body	The cloud service provider informs personnel and external business partners of their obligations. If necessary, they agree to or are contractually obliged to timely report all security events that become known to them and are directly related to the cloud service provided by the cloud service provider to a previously designated central office of the cloud service provider.	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	5		IRO-11
SIM-05.02B	Duty of the Personnel to Report Security Incidents to a Central Body	The cloud service provider communicates that 'false reports' of events that do not subsequently turn out to be incidents do not have any negative consequences.	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	3		IRO-11
SIM-05.03B	Duty of the Personnel to Report Security Incidents to a Central Body	The information security incident reporting mechanisms are communicated to personnel, cloud service customers and service organisations of the cloud service provider.	Functional	Intersects With	Incident Reporting Assistance	IRO-18	Mechanisms exist to provide incident response advice and assistance to users of Technology Assets, Applications and/or Services (TAAS) for the handling and reporting of actual and potential cybersecurity and data protection incidents.	5		IRO-11
SIM-06.01B	Evaluation and Learning Process	Mechanisms are in place to measure and monitor the type and scope of security incidents and to report them to supporting bodies.	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	3		GOV-05
SIM-06.01B	Evaluation and Learning Process	Mechanisms are in place to measure and monitor the type and scope of security incidents and to report them to supporting bodies.	Functional	Intersects With	Situational Awareness For Incidents	IRO-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5		IRO-09
SIM-06.02B	Evaluation and Learning Process	The cloud service provider defines, implements and maintains a knowledge repository containing:	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5		IRO-13
SIM-06.02B.1	Evaluation and Learning Process	Security incidents;	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
SIM-06.02B.2	Evaluation and Learning Process	Measures taken for the solution of these security incidents; and	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
SIM-06.02B.3	Evaluation and Learning Process	Information about the assets affected by these security incidents.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	3		IRO-13
SIM-06.02B.4	Evaluation and Learning Process	This information is used to supplement the classification catalogue of incidents (cf. SIM-03).	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	3		IRO-02.4
SIM-06.03B	Evaluation and Learning Process	The information obtained from the security incident monitoring and the intelligence gathered in the knowledge repository is used to identify recurring security events or security incidents, or potential significant security incidents, to determine the need for advanced safeguards, and for implementing them.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5		IRO-13
SIM-06.03B	Evaluation and Learning Process	The information obtained from the security incident monitoring and the intelligence gathered in the knowledge repository is used to identify recurring security events or security incidents, or potential significant security incidents, to determine the need for advanced safeguards, and for implementing them.	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	3		THR-10
SIM-06.04B	Evaluation and Learning Process	The evaluation and learning process includes the results of root-cause analyses conducted in accordance with SIM-03.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5		IRO-13

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
5.14	Business Continuity Management (BCM)	Objective: Plan, implement, maintain and test procedures and measures for business continuity and emergency management.	Functional	Intersects With	Business Continuity & Disaster Recovery Policy	BCD-01	Mechanisms exist to establish a formal, documented Business Continuity and Disaster Recovery (BC/DR) policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving	5		
5.14	Business Continuity Management (BCM)	Objective: Plan, implement, maintain and test procedures and measures for business continuity and emergency management.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and	10		BCD-01
BCM-01.01B	Business Continuity and Emergency Management System	The cloud service provider operates a business continuity and emergency management system in accordance with ISO 22301 and/or BSI 200-4.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	8		BCD-01
BCM-01.01B	Business Continuity and Emergency Management System	The cloud service provider operates a business continuity and emergency management system in accordance with ISO 22301 and/or BSI 200-4.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-03.1	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and (2) Provide defensible justification for secure	3		GOV-01.4
BCM-01.02B	Business Continuity and Emergency Management System	Policies and procedures for the cloud service's business continuity management, including strategy and guidelines, business impact analyses, and business continuity plans, are documented, communicated, and made available in accordance with SP-01 regarding the following aspects:	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	5		BCD-01
BCM-01.02B	Business Continuity and Emergency Management System	Policies and procedures for the cloud service's business continuity management, including strategy and guidelines, business impact analyses, and business continuity plans, are documented, communicated, and made available in accordance with SP-01 regarding the following aspects:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
BCM-01.02B	Business Continuity and Emergency Management System	Policies and procedures for the cloud service's business continuity management, including strategy and guidelines, business impact analyses, and business continuity plans, are documented, communicated, and made available in accordance with SP-01 regarding the following aspects:	Functional	Intersects With	Business Continuity & Disaster Recovery Policy	BCD-01	Mechanisms exist to establish a formal, documented Business Continuity and Disaster Recovery (BC/DR) policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving	8		
BCM-01.02B.1	Business Continuity and Emergency Management System	Goals of the BCM;	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
BCM-01.02B.2	Business Continuity and Emergency Management System	Roles and responsibilities, management commitment;	Functional	Intersects With	Recovery Operations Criteria	BCD-05	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recovery (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-01.5
BCM-01.02B.3	Business Continuity and Emergency Management System	Scoping of the BCM, identifying relevant business processes;	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5		BCD-02
BCM-01.02B.4	Business Continuity and Emergency Management System	Interfaces, in particular to Incident Management;	Functional	Intersects With	Coordinate with Related Plans	BCD-07.3	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5		BCD-01.1
BCM-01.02B.4	Business Continuity and Emergency Management System	Interfaces, in particular to Incident Management;	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	3		IRO-04
BCM-01.02B.5	Business Continuity and Emergency Management System	Communication with relevant entities and competent authorities;	Functional	Intersects With	Contingency Plan Update Notifications	BCD-07.2	Mechanisms exist to keep stakeholders informed of changes to contingency plans.	3		BCD-06.2
BCM-01.02B.5	Business Continuity and Emergency Management System	Communication with relevant entities and competent authorities;	Functional	Intersects With	Contacts With Authorities	GOV-15	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	3		GOV-06
BCM-01.02B.6	Business Continuity and Emergency Management System	Methodology;	Functional	Intersects With	Business Continuity & Disaster Recovery Policy	BCD-01	Mechanisms exist to establish a formal, documented Business Continuity and Disaster Recovery (BC/DR) policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors;	5		
BCM-01.02B.6	Business Continuity and Emergency Management System	Methodology;	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
BCM-01.02B.7	Business Continuity and Emergency Management System	Consideration of Risk;	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
BCM-01.02B.8	Business Continuity and Emergency Management System	Business Impact Analysis (BIA);	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5		RSK-08
BCM-01.02B.9	Business Continuity and Emergency Management System	Business Continuity Plan (BCP);	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	5		BCD-01
BCM-01.02B.10	Business Continuity and Emergency Management System	Resource Planning (usually part of the BCP);	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
BCM-01.02B.10	Business Continuity and Emergency Management System	Resource Planning (usually part of the BCP);	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	3		PRM-03
BCM-01.02B.11	Business Continuity and Emergency Management System	Testing of Business Continuity Plans and regular updates to BCM documentation; and	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
BCM-01.02B.12	Business Continuity and Emergency Management System	Continuous improvement of the Business Continuity Management.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-11	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	3		BCD-05

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
BCM-01.03B	Business Continuity and Emergency Management System	The top management (or a member of the top management) of the cloud service provider is named as the process owner of business continuity and emergency management and is responsible for establishing the process within the company as well as ensuring compliance with the guidelines. They ensure that sufficient resources are made available for an effective process.	Functional	Intersects With	Recovery Operations Criteria	BCD-05	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recovery (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-01.5
BCM-01.03B	Business Continuity and Emergency Management System	The top management (or a member of the top management) of the cloud service provider is named as the process owner of business continuity and emergency management and is responsible for establishing the process within the company as well as ensuring compliance with the guidelines. They ensure that sufficient resources are made available for an effective process.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	3		GOV-04
BCM-01.04B	Business Continuity and Emergency Management System	People in management and other relevant leadership positions demonstrate leadership and commitment to this issue by encouraging personnel to actively contribute to the effectiveness of continuity and emergency management.	Functional	Intersects With	Recovery Operations Criteria	BCD-05	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recovery (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-01.5
BCM-01.04B	Business Continuity and Emergency Management System	People in management and other relevant leadership positions demonstrate leadership and commitment to this issue by encouraging personnel to actively contribute to the effectiveness of continuity and emergency management.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3		GOV-01.2
BCM-02.01B	Business Impact Analysis	The cloud service provider performs a Business Impact Analysis (BIA). In this BIA, the cloud service provider analyses the impact of disrupting activities to its organisation with respect the development and operations of the cloud service in accordance with applicable policies and procedures with at least the following aspects:	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5		BCD-02
BCM-02.01B	Business Impact Analysis	The cloud service provider performs a Business Impact Analysis (BIA). In this BIA, the cloud service provider analyses the impact of disrupting activities to its organisation with respect the development and operations of the cloud service in accordance with applicable policies and procedures with at least the following aspects:	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	8		RSK-08
BCM-02.01B.1	Business Impact Analysis	Possible scenarios based on a risk assessment that includes cybersecurity risks;	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	3		RSK-08
BCM-02.01B.1	Business Impact Analysis	Possible scenarios based on a risk assessment that includes cybersecurity risks;	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	3		RSK-03
BCM-02.01B.2	Business Impact Analysis	Identification of critical products and services;	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5		BCD-02
BCM-02.01B.3	Business Impact Analysis	Identification of dependencies, including processes (including resources required), applications, business partners and third parties;	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	3		BCD-02
BCM-02.01B.3	Business Impact Analysis	Identification of dependencies, including processes (including resources required), applications, business partners and third parties;	Functional	Intersects With	Third-Party Criticality Assessments	TPM-09	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	3		TPM-02
BCM-02.01B.4	Business Impact Analysis	Capturing threats to critical products and services;	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	3		RSK-08
BCM-02.01B.4	Business Impact Analysis	Capturing threats to critical products and services;	Functional	Intersects With	Threat Catalog	THR-06	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	3		THR-09
BCM-02.01B.5	Business Impact Analysis	Identification of effects resulting from planned and unplanned outages, service degradations and changes over time;	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	3		RSK-08
BCM-02.01B.6	Business Impact Analysis	Determination of the maximum tolerable period of downtime and service degregation;	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-01.4
BCM-02.01B.7	Business Impact Analysis	Identification of restoration priorities;	Functional	Intersects With	Resume All Missions & Business Functions	BCD-08	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5		BCD-02.1
BCM-02.01B.8	Business Impact Analysis	Determination of time targets for the resumption of critical products and services within the maximum acceptable time period (i.e. RTO);	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8		BCD-01.4
BCM-02.01B.9	Business Impact Analysis	Determination of time targets for the maximum reasonable period during which cloud service derived data, cloud service provider data, account data and, if its processing is contractually agreed upon, cloud service customer data can be lost and not recovered (i.e. RPO); and	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8		BCD-01.4
BCM-02.01B.10	Business Impact Analysis	Estimation of the resources needed for resumption.	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	3		PRM-03
BCM-02.01B.10	Business Impact Analysis	Estimation of the resources needed for resumption.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	3		RSK-08
BCM-02.02B	Business Impact Analysis	The business impact analysis adheres to the applicable policies and procedures and is reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5		RSK-08
BCM-03.01B	Business Continuity Plans	Based on the results of the business impact analysis, business continuity plans are documented in a consistent manner, and in accordance with applicable policies and procedures. Business continuity plans take the following aspects into account:	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	8		BCD-01
BCM-03.01B.1	Business Continuity Plans	Defined purpose and scope with consideration of the relevant dependencies;	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
BCM-03.01B.2	Business Continuity Plans	Accessibility and comprehensibility of the plans for persons who are to act accordingly;	Functional	Intersects With	Contingency Training	BCD-09	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	3		BCD-03
BCM-03.01B.3	Business Continuity Plans	Ownership by at least one designated person responsible for review, updating and approval;	Functional	Intersects With	Ongoing Contingency Planning	BCD-07	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services); (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing	3		BCD-06
BCM-03.01B.3	Business Continuity Plans	Ownership by at least one designated person responsible for review, updating and approval;	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	3		GOV-04

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
BCM-03.01B.4	Business Continuity Plans	Defined communication channels, roles and responsibilities including notification of the customer;	Functional	Intersects With	Recovery Operations Criteria	BCD-05	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recovery (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-01.5
BCM-03.01B.4	Business Continuity Plans	Defined communication channels, roles and responsibilities including notification of the customer;	Functional	Intersects With	Contingency Plan Update Notifications	BCD-07.2	Mechanisms exist to keep stakeholders informed of changes to contingency plans.	3		BCD-06.2
BCM-03.01B.5	Business Continuity Plans	Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of cloud hardware objects and services and alignment with customers);	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
BCM-03.01B.5	Business Continuity Plans	Recovery procedures, manual interim solutions and reference information (taking into account prioritisation in the recovery of cloud hardware objects and services and alignment with customers);	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-08.1	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration of primary processing and/or storage sites is performed.	5		BCD-02.2
BCM-03.01B.6	Business Continuity Plans	Methods for putting the plans into effect;	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
BCM-03.01B.7	Business Continuity Plans	Continuous process improvement;	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-11	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	3		BCD-05
BCM-03.01B.8	Business Continuity Plans	Consistency over all locations, zones, regions and partitions; and	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	3		BCD-01
BCM-03.01B.9	Business Continuity Plans	Interfaces to Security Incident Management.	Functional	Intersects With	Coordinate with Related Plans	BCD-07.3	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5		BCD-01.1
BCM-03.01B.9	Business Continuity Plans	Interfaces to Security Incident Management.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	3		IRO-04
BCM-03.02B	Business Continuity Plans	The business continuity plans are reviewed at regular intervals, at least once a year, or after significant organisational or environment-related changes.	Functional	Intersects With	Ongoing Contingency Planning	BCD-07	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services); (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing	5		BCD-06
BCM-04.01B	Testing Business Continuity	Business continuity plans are tested on a regular basis (at least annually) or after significant organisational or environmental changes. Tests involve affected cloud service customers and relevant third parties (e.g. service organisations).	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	8		BCD-04
BCM-04.01B	Testing Business Continuity	Business continuity plans are tested on a regular basis (at least annually) or after significant organisational or environmental changes. Tests involve affected cloud service customers and relevant third parties (e.g. service organisations).	Functional	Intersects With	Coordinated Testing with Related Plans	BCD-10.1	Mechanisms exist to coordinate contingency plan testing with internal and external parties responsible for related plans.	5		BCD-04.1
BCM-04.02B	Testing Business Continuity	The tests are documented and results are taken into account to review the business continuity plans and for future business continuity measures.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
BCM-04.02B	Testing Business Continuity	The tests are documented and results are taken into account to review the business continuity plans and for future business continuity measures.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-11	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	3		BCD-05
BCM-04.01AC	Testing Business Continuity	In addition to the tests, exercises are also carried out which, among other things, have resulted in scenarios from security incidents that have already occurred in the past.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	3		BCD-04
BCM-04.01AC	Testing Business Continuity	In addition to the tests, exercises are also carried out which, among other things, have resulted in scenarios from security incidents that have already occurred in the past.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
BCM-04.02AC	Testing Business Continuity	The cloud service provider has procedures in place to ensure that cloud service customers are timely informed about planned activities related to business continuity tests and exercises that could affect the information security of the cloud service (e.g. regarding its availability). This information includes the scheduled time frame for the operations as well as a description of the work to be carried out.	Functional	Intersects With	Coordinated Testing with Related Plans	BCD-10.1	Mechanisms exist to coordinate contingency plan testing with internal and external parties responsible for related plans.	3		BCD-04.1
BCM-04.02AC	Testing Business Continuity	The cloud service provider has procedures in place to ensure that cloud service customers are timely informed about planned activities related to business continuity tests and exercises that could affect the information security of the cloud service (e.g. regarding its availability). This information includes the scheduled time frame for the operations as well as a description of the work to be carried out.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	3		CHG-05
BCM-04.03AC	Testing Business Continuity	The cloud service provider provides cloud service customers an assessment of the potential impacts of those tests and excercises concerning the information security of the cloud service and with details for contacting the cloud service provider.	Functional	Intersects With	Coordinated Testing with Related Plans	BCD-10.1	Mechanisms exist to coordinate contingency plan testing with internal and external parties responsible for related plans.	3		BCD-04.1
BCM-04.04AC	Testing Business Continuity	After a completed exercise, the existing alarm and notification plan is reviewed and (if needed) adapted.	Functional	Intersects With	Ongoing Contingency Planning	BCD-07	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services); (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing	3		BCD-06
BCM-04.04AC	Testing Business Continuity	After a completed exercise, the existing alarm and notification plan is reviewed and (if needed) adapted.	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-15	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	3		IRO-14
5.15	Compliance (COM)	Objective: Avoid non-compliance with legal, regulatory, self-imposed or contractual information security and compliance requirements.	Functional	No Relationship	N/A	N/A	N/A	0		
COM-01.01B	Identification of Applicable Legal, Regulatory, Self-imposed or Contractual	The legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service as well as the cloud service provider's procedures for complying with these requirements are explicitly defined and documented.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	8		CPL-01
COM-01.01AC	Identification of Applicable Legal, Regulatory, Self-imposed or Contractual Requirements	The cloud service provider provides an overview of the procedures described in the basic criterion upon request by the cloud service customer.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
COM-02.01B	Policy for Planning and Conducting Audits	The cloud service provider documents and implements an audit programme over multiple years that defines the scope and the frequency of the audits. The audit programme takes into consideration the management of change, policies, and the results of the risk assessment (cf. OIS-07).	Functional	Intersects With	Executive Leadership Oversight of Security, Compliance & Resilience Controls	CPL-07	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5		CPL-02
COM-02.01B	Policy for Planning and Conducting Audits	The cloud service provider documents and implements an audit programme over multiple years that defines the scope and the frequency of the audits. The audit programme takes into consideration the management of change, policies, and the results of the risk assessment (cf. OIS-07).	Functional	Intersects With	Information Assurance (IA) Operations	IAO-02	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	3		IAO-01
COM-02.02B	Policy for Planning and Conducting Audits	Risk-based policies and procedures for planning and conducting audits are documented, communicated and made available in accordance with SP-01 and address the following aspects in order to prevent adversal effects on the operation of the cloud service from the audit:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8		GOV-02
COM-02.02B.1	Policy for Planning and Conducting Audits	Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities;	Functional	Intersects With	Executive Leadership Oversight of Security, Compliance & Resilience Controls	CPL-07	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	3		CPL-02
COM-02.02B.1	Policy for Planning and Conducting Audits	Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities;	Functional	Intersects With	Audit Planning Activities	CPL-07.3	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	5		CPL-04
COM-02.02B.1	Policy for Planning and Conducting Audits	Restriction to read-only access to system components in accordance with the agreed audit plan and as necessary to perform the activities;	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business	3		IAC-21
COM-02.02B.2	Policy for Planning and Conducting Audits	Activities that may result in outages, degradations of the cloud service or breaches of contractual requirements are performed during scheduled maintenance windows or outside peak periods;	Functional	Intersects With	Executive Leadership Oversight of Security, Compliance & Resilience Controls	CPL-07	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	3		CPL-02
COM-02.02B.3	Policy for Planning and Conducting Audits	Logging and monitoring of activities;	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
COM-02.02B.4	Policy for Planning and Conducting Audits	Review of server and network equipment configurations under the responsibility of the cloud service provider;	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5		CPL-03.2
COM-02.02B.5	Policy for Planning and Conducting Audits	Intrusion testing for external access points; and	Functional	Intersects With	External Vulnerability Assessment	VPM-14	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).	3		VPM-06.6
COM-02.02B.5	Policy for Planning and Conducting Audits	Intrusion testing for external access points; and	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
COM-02.02B.6	Policy for Planning and Conducting Audits	Source code reviews of internally developed security features.	Functional	Intersects With	Static Code Analysis	TDA-17.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	5		TDA-09.2
COM-02.01AS	Policy for Planning and Conducting Audits	COM-02.01AS, sharpening COM-02.01B The cloud service provider documents and implements an audit programme over three years that defines the scope and the frequency of the audits. The audit programme takes into consideration the management of change, policies, and the results of the risk assessment (cf. OIS-07).	Functional	Intersects With	Executive Leadership Oversight of Security, Compliance & Resilience Controls	CPL-07	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5		CPL-02
COM-02.01AC	Policy for Planning and Conducting Audits	The cloud service provider grants its cloud service customers contractually agreed information and audit rights. These rights may be exercised individually or as part of group audits.	Functional	Intersects With	Executive Leadership Oversight of Security, Compliance & Resilience Controls	CPL-07	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	3		CPL-02
COM-02.01AC	Policy for Planning and Conducting Audits	The cloud service provider grants its cloud service customers contractually agreed information and audit rights. These rights may be exercised individually or as part of group audits.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
COM-03.01B	Internal Audits of the Information Security Management System	Subject matter experts check the compliance of the information security management system at regular intervals, at least annually, with the relevant and applicable legal, regulatory, self-imposed or contractual requirements (cf. COM-01) through internal audits. This includes checks regarding:	Functional	Intersects With	Conformity Monitoring	CPL-05	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	3		CPL-03
COM-03.01B	Internal Audits of the Information Security Management System	Subject matter experts check the compliance of the information security management system at regular intervals, at least annually, with the relevant and applicable legal, regulatory, self-imposed or contractual requirements (cf. COM-01) through internal audits. This includes checks regarding:	Functional	Intersects With	Executive Leadership Oversight of Security, Compliance & Resilience Controls	CPL-07	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	8		CPL-02
COM-03.01B.1	Internal Audits of the Information Security Management System	Compliance with the policies and procedures (cf. SP-01) within their scope of responsibility (cf. OIS-01); and	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5		CPL-03.2
COM-03.01B.2	Internal Audits of the Information Security Management System	Effectiveness of organisational and operational measures to manage the risks posed to the security of network and information systems (cf. OIS-07).	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5		IAO-02
COM-03.01B.2	Internal Audits of the Information Security Management System	Effectiveness of organisational and operational measures to manage the risks posed to the security of network and information systems (cf. OIS-07).	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
COM-03.02B	Internal Audits of the Information Security Management System	Subject matter experts conducting internal audits are not in the line of authority of the personnel of the area under review. If the size of the cloud service provider does not allow such separation of line of authority, alternative measures to guarantee the impartiality of compliance checks are put in place.	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	8		CPL-02.1
COM-03.03B	Internal Audits of the Information Security Management System	Identified vulnerabilities and deviations as well as non-conformities from the applicable legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service, are subjected to a risk assessment in accordance with the risk management procedure (cf. OIS-07). Follow-up measures are defined and tracked (cf. OPS-18).	Functional	Intersects With	Non-Conformity Oversight	CPL-06	Mechanisms exist to identify and document instances of non-conformity with statutory, regulatory and/or contractual obligations, in order to develop appropriate risk mitigation actions.	5		CPL-01.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
COM-03.03B	Internal Audits of the Information Security Management System	Identified vulnerabilities and deviations as well as non-conformities from the applicable legal, regulatory, self-imposed and contractual requirements relevant to the information security of the cloud service, are subjected to a risk assessment in accordance with the risk management procedure (cf. OIS-07). Follow-up measures are defined and tracked (cf. OPS-18).	Functional	Intersects With	Risk Response	RSK-16	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.	3		RSK-06.1
COM-03.01AC	Internal Audits of the Information Security Management System	Based on a risk assessment (cf. OIS-07) and technical feasibility, the cloud service provider decides to which extent internal audits are supplemented by procedures to automatically monitor applicable requirements of policies and procedures with regard to the following aspects:	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	3		CFG-06
COM-03.01AC	Internal Audits of the Information Security Management System	Based on a risk assessment (cf. OIS-07) and technical feasibility, the cloud service provider decides to which extent internal audits are supplemented by procedures to automatically monitor applicable requirements of policies and procedures with regard to the following aspects:	Functional	Intersects With	Conformity Monitoring	CPL-05	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5		CPL-03
COM-03.01AC.1	Internal Audits of the Information Security Management System	Configuration of system components to provide the cloud service within the cloud service provider's area of responsibility;	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-08.2	Automated mechanisms exist to: (1) Identify unauthorized deviations from an approved secure baseline configuration; and (2) Implement automated resiliency actions to remediate the unauthorized change.	5		CFG-06
COM-03.01AC.2	Internal Audits of the Information Security Management System	Performance and availability of these system components;	Functional	Intersects With	Performance Monitoring	CAP-05	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical Technology Assets, Applications and/or Services (TAAS).	3		CAP-04
COM-03.01AC.3	Internal Audits of the Information Security Management System	Response time to incidents and security incidents; and	Functional	Intersects With	Situational Awareness For Incidents	IRO-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	3		IRO-09
COM-03.01AC.4	Internal Audits of the Information Security Management System	Recovery time (time to completion of error handling).	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-01.4
COM-03.02AC	Internal Audits of the Information Security Management System	Identified vulnerabilities and deviations are automatically reported to the appropriate cloud service provider's subject matter experts for immediate assessment and action.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
COM-03.02AC	Internal Audits of the Information Security Management System	Identified vulnerabilities and deviations are automatically reported to the appropriate cloud service provider's subject matter experts for immediate assessment and action.	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	3		MON-01.4
COM-03.03AC	Internal Audits of the Information Security Management System	The cloud service provider provides interfaces to cloud service customers so that they can check compliance with selected contractual agreements in real time.	Functional	Intersects With	Conformity Monitoring	CPL-05	Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	3		CPL-03
COM-04.01B	Information on Information Security Performance and Management Assessment of the ISMS	The top management of the cloud service provider is regularly informed about the information security performance within the scope of the ISMS in order to ensure its continued suitability, adequacy and effectiveness. The information is included in the management review of the ISMS. This management review is performed at least once a year.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	8		GOV-01.2
COM-04.01B	Information on Information Security Performance and Management Assessment of the ISMS	The top management of the cloud service provider is regularly informed about the information security performance within the scope of the ISMS in order to ensure its continued suitability, adequacy and effectiveness. The information is included in the management review of the ISMS. This management review is performed at least once a year.	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	3		GOV-05
COM-04.01AC	Information on Information Security Performance and Management Assessment of the ISMS	The cloud service provider defines and implements technical and operational metrics that align with the organisation's business objectives, security requirements, and compliance obligations. These metrics are documented and included in the management review of the ISMS to ensure their continued suitability, adequacy, and effectiveness.	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	8		GOV-05
COM-04.01AC	Information on Information Security Performance and Management Assessment of the ISMS	The cloud service provider defines and implements technical and operational metrics that align with the organisation's business objectives, security requirements, and compliance obligations. These metrics are documented and included in the management review of the ISMS to ensure their continued suitability, adequacy, and effectiveness.	Functional	Intersects With	Key Performance Indicators (KPIs)	GOV-12.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring, trend analysis, and possible control redesign or replacement for the Security, Compliance & Resilience Program (SCRP).	5		GOV-05.1
COM-04.02AC	Information on Information Security Performance and Management Assessment of the ISMS	The responsible business units of the cloud service provider report at least annually to the top management on the the status and effectiveness of the policies and procedures that are relevant to the top management review of the information security management system. This reporting includes at least:	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2
COM-04.02AC.1	Information on Information Security Performance and Management Assessment of the ISMS	Implemented changes to address cybersecurity risks for the topic addressed in the policy or procedure;	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3		GOV-01.2
COM-04.02AC.2	Information on Information Security Performance and Management Assessment of the ISMS	Information security incidents for the topic addressed in the policy or procedure and the follow-up;	Functional	Intersects With	Situational Awareness For Incidents	IRO-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	3		IRO-09
COM-04.02AC.3	Information on Information Security Performance and Management Assessment of the ISMS	Performance of the internal controls regarding information security for the topic addressed in the policy or procedure; and	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	3		GOV-05
COM-04.02AC.4	Information on Information Security Performance and Management Assessment of the ISMS	Planned changes for the topic addressed in the policy or procedure to address cybersecurity risks and information security and cybersecurity.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3		GOV-01.2
5.16	Dealing with Investigation Requests from Government Agencies (INQ)	Objective: Ensure appropriate handling of government investigation requests for legal review, information to cloud service customers, and limitation of access to or disclosure of data.	Functional	No Relationship	N/A	N/A	N/A	0		

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
INQ-01.01B	Legal Assessment of Investigation Requests	Investigation requests from government agencies for cloud service customer data, cloud service derived data and account data are subject to a documented legal assessment by subject matter experts of the cloud service provider. The assessment determines whether the government agency has an applicable and legally valid legal basis and what further steps need to be taken for the given request.	Functional	Intersects With	Government Surveillance	CPL-20	Mechanisms exist to constrain the host government from having unrestricted and unmonitored access to the organization's Technology Assets, Applications, Services and/or Data (TAASD) that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	5		CPL-06
INQ-01.01B	Legal Assessment of Investigation Requests	Investigation requests from government agencies for cloud service customer data, cloud service derived data and account data are subject to a documented legal assessment by subject matter experts of the cloud service provider. The assessment determines whether the government agency has an applicable and legally valid legal basis and what further steps need to be taken for the given request.	Functional	Intersects With	Notification of Disclosure Requests To Data Subject	PRI-18	Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).	3		PRI-14.2
INQ-01.02B	Legal Assessment of Investigation Requests	Access to or disclosure of cloud service customer data, cloud service derived data or account data in response to government investigation requests is only permitted if the cloud service provider has performed a legal assessment. This assessment has to confirm that there is an applicable and valid legal basis and that the request must be granted according to this basis.	Functional	Intersects With	Government Surveillance	CPL-20	Mechanisms exist to constrain the host government from having unrestricted and unmonitored access to the organization's Technology Assets, Applications, Services and/or Data (TAASD) that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	5		CPL-06
INQ-02.01B	Informing Cloud Service Customers about Investigation Requests	The cloud service provider informs the affected cloud service customer(s) without undue delay, unless the applicable legal basis, on which the government agency's request is based, prohibits this or there are clear indications of illegal actions in connection with the use of the cloud service.	Functional	Intersects With	Government Surveillance	CPL-20	Mechanisms exist to constrain the host government from having unrestricted and unmonitored access to the organization's Technology Assets, Applications, Services and/or Data (TAASD) that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	3		CPL-06
INQ-02.01B	Informing Cloud Service Customers about Investigation Requests	The cloud service provider informs the affected cloud service customer(s) without undue delay, unless the applicable legal basis, on which the government agency's request is based, prohibits this or there are clear indications of illegal actions in connection with the use of the cloud service.	Functional	Intersects With	Notification of Disclosure Requests To Data Subject	PRI-18	Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).	5		PRI-14.2
INQ-03.01B	Limiting Access to or Disclosure of Data in Investigation Requests	The cloud service provider's procedures for granting access to or disclosing cloud service customer data and cloud service derived data in the context of investigation requests from government agencies ensure that the agencies only gain access to or insight into the data that is the subject of the investigation request.	Functional	Intersects With	Government Surveillance	CPL-20	Mechanisms exist to constrain the host government from having unrestricted and unmonitored access to the organization's Technology Assets, Applications, Services and/or Data (TAASD) that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	5		CPL-06
INQ-03.01B	Limiting Access to or Disclosure of Data in Investigation Requests	The cloud service provider's procedures for granting access to or disclosing cloud service customer data and cloud service derived data in the context of investigation requests from government agencies ensure that the agencies only gain access to or insight into the data that is the subject of the investigation request.	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	3		IAC-21
INQ-03.02B	Limiting Access to or Disclosure of Data in Investigation Requests	If no clear limitation of the cloud service customer data and cloud service derived data is possible, the cloud service provider anonymises or pseudonymises this data so that government agencies can only assign it to those cloud service customers who are subject of the investigation request.	Functional	Intersects With	De-Identification (Anonymization)	DCH-36	Mechanisms exist to de-identify sensitive and/or regulated data through (1) Anonymization; (2) De-identification; (3) Pseudonymization; and/or (4) Redaction.	5		DCH-23
INQ-03.01AC	Limiting Access to or Disclosure of Data in Investigation Requests	The access and activities performed by or on behalf of investigators are monitored by the cloud service provider as determined by the process described in INQ-01.	Functional	Intersects With	Government Surveillance	CPL-20	Mechanisms exist to constrain the host government from having unrestricted and unmonitored access to the organization's Technology Assets, Applications, Services and/or Data (TAASD) that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	3		CPL-06
INQ-03.01AC	Limiting Access to or Disclosure of Data in Investigation Requests	The access and activities performed by or on behalf of investigators are monitored by the cloud service provider as determined by the process described in INQ-01.	Functional	Intersects With	Audit Trails	MON-09.1	Mechanisms exist to link system access to individual users or service accounts.	3		MON-03.2
INQ-03.02AC	Limiting Access to or Disclosure of Data in Investigation Requests	Timely and appropriate remediation measures address any deviations identified during the monitoring of the activities performed by or on behalf of investigators.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
INQ-04.01B	Communication of Technical Procedures for Data Disclosure in Investigation Requests	The cloud service provider documents the technical procedures per service and other technical information regarding the provision or disclosure of cloud service customer data in response to valid investigation requests and provides it to cloud service customers.	Functional	Intersects With	Government Surveillance	CPL-20	Mechanisms exist to constrain the host government from having unrestricted and unmonitored access to the organization's Technology Assets, Applications, Services and/or Data (TAASD) that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	3		CPL-06
INQ-04.01B	Communication of Technical Procedures for Data Disclosure in Investigation Requests	The cloud service provider documents the technical procedures per service and other technical information regarding the provision or disclosure of cloud service customer data in response to valid investigation requests and provides it to cloud service customers.	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04
INQ-04.02B	Communication of Technical Procedures for Data Disclosure in Investigation Requests	The type and scope of the information provided to the cloud service customers is based on the needs of their expert personnel to assess risks to the cloud service customer's data confidentiality. At a minimum, the following aspects are addressed:	Functional	Intersects With	Government Surveillance	CPL-20	Mechanisms exist to constrain the host government from having unrestricted and unmonitored access to the organization's Technology Assets, Applications, Services and/or Data (TAASD) that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	3		CPL-06
INQ-04.02B.1	Communication of Technical Procedures for Data Disclosure in Investigation Requests	The process for the provision and disclosure of cloud service customer data in response to legitimate investigation requests;	Functional	Intersects With	Government Surveillance	CPL-20	Mechanisms exist to constrain the host government from having unrestricted and unmonitored access to the organization's Technology Assets, Applications, Services and/or Data (TAASD) that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	3		CPL-06
INQ-04.02B.2	Communication of Technical Procedures for Data Disclosure in Investigation Requests	The technical capabilities and limitations of the cloud service provider regarding disclosure of cloud service customer data;	Functional	Intersects With	Government Surveillance	CPL-20	Mechanisms exist to constrain the host government from having unrestricted and unmonitored access to the organization's Technology Assets, Applications, Services and/or Data (TAASD) that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	3		CPL-06
INQ-04.02B.3	Communication of Technical Procedures for Data Disclosure in Investigation Requests	Logging mechanisms implemented to records access for disclosure of cloud service customer data;	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
INQ-04.02B.4	Communication of Technical Procedures for Data Disclosure in Investigation Requests	Access possibilities for cloud service customers to review such logs;	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-07.1	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	3		CLD-06.2
INQ-04.02B.5	Communication of Technical Procedures for Data Disclosure in Investigation Requests	Methods and technical procedures per service for accessing and disclosing cloud service customer data; and	Functional	Intersects With	Government Surveillance	CPL-20	Mechanisms exist to constrain the host government from having unrestricted and unmonitored access to the organization's Technology Assets, Applications, Services and/or Data (TAASD) that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	3		CPL-06
INQ-04.02B.6	Communication of Technical Procedures for Data Disclosure in Investigation Requests	Laws, regulations, or other legal means and their applicability concerning the cloud service provider's ability to inform its customers about the provision and disclosure of cloud service customer data.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
INQ-04.03B	Communication of Technical Procedures for Data Disclosure in Investigation Requests	The aforementioned document is maintained in accordance with SP-01 and aligned with the cloud service provider's guidelines on minimising access to cloud service customer data (cf. DEV-01) to ensure its relevance and accuracy for cloud service customers.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
5.17	Product Safety and Security (PSS)	Objective: Provide up-to-date information on the secure configuration and known vulnerabilities of the cloud service for cloud service customers, appropriate mechanisms for troubleshooting and logging, as well as authentication and authorisation of users of cloud service customers.	Functional	No Relationship	N/A	N/A	N/A	0		
PSS-01.01B	Guidelines and Recommendations for Cloud Service Customers	The cloud service provider publishes guidelines and recommendations for cloud service customers regarding the secure use of the cloud service provided. The information contained therein is intended to assist the cloud service customer in the secure configuration and use of the cloud service, as well as the implementation of complementary customer controls, to the extent applicable to the cloud service and the responsibility of the cloud service customer.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	3		CLD-06.1
PSS-01.01B	Guidelines and Recommendations for Cloud Service Customers	The cloud service provider publishes guidelines and recommendations for cloud service customers regarding the secure use of the cloud service provided. The information contained therein is intended to assist the cloud service customer in the secure configuration and use of the cloud service, as well as the implementation of complementary customer controls, to the extent applicable to the cloud service and the responsibility of the cloud service customer.	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5		TDA-04
PSS-01.02B	Guidelines and Recommendations for Cloud Service Customers	The type and scope of the information in the guidelines and recommendations for the secure use of the cloud service provided will be based on the needs of subject matter experts of the cloud service customers who set information security requirements, implement them or verify the implementation (e.g. IT, Compliance, Internal Audit). The information in the guidelines and recommendations for the secure use of the cloud service address the following aspects, where applicable to the cloud service:	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5		TDA-04
PSS-01.02B.1	Guidelines and Recommendations for Cloud Service Customers	Procedures for secure configuration;	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
PSS-01.02B.2	Guidelines and Recommendations for Cloud Service Customers	Information sources on known vulnerabilities and update mechanisms;	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	3		VPM-01
PSS-01.02B.3	Guidelines and Recommendations for Cloud Service Customers	Malware protection for containers or virtual machines;	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	3		END-04
PSS-01.02B.4	Guidelines and Recommendations for Cloud Service Customers	Error handling and logging mechanisms;	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
PSS-01.02B.5	Guidelines and Recommendations for Cloud Service Customers	Authentication mechanisms;	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	3		IAC-10
PSS-01.02B.6	Guidelines and Recommendations for Cloud Service Customers	Roles and rights framework including combinations that result in an elevated risk;	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	3		IAC-08
PSS-01.02B.7	Guidelines and Recommendations for Cloud Service Customers	Services and functions for administration of the cloud service by privileged users;	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	3		IAC-16
PSS-01.02B.8	Guidelines and Recommendations for Cloud Service Customers	Complementary user entity controls;	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	5		CLD-06.1
PSS-01.02B.9	Guidelines and Recommendations for Cloud Service Customers	Encryption mechanisms and services;	Functional	Intersects With	Use of Cryptographic Controls	CRY-02	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	3		CRY-01
PSS-01.02B.10	Guidelines and Recommendations for Cloud Service Customers	Data leakage prevention;	Functional	Intersects With	Data Loss Prevention (DLP)	DCH-40	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	3		NET-17
PSS-01.02B.11	Guidelines and Recommendations for Cloud Service Customers	Secure application development and operation on the cloud service;	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3		TDA-06
PSS-01.02B.12	Guidelines and Recommendations for Cloud Service Customers	Instructions for using and configuring defensive mechanisms;	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
PSS-01.02B.13	Guidelines and Recommendations for Cloud Service Customers	Instructions for using and configuring wide-area distributed architecture mechanisms;	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04
PSS-01.02B.14	Guidelines and Recommendations for Cloud Service Customers	Methods used for client data separation (cf. OPS-30 and OPS-31);	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	3		CLD-06
PSS-01.02B.15	Guidelines and Recommendations for Cloud Service Customers	How information security risks related to the use of the cloud service can be addressed through proper logging and monitoring mechanisms; and	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
PSS-01.02B.16	Guidelines and Recommendations for Cloud Service Customers	Inbound and outbound interfaces through which the cloud service can be accessed by other cloud services or IT systems of cloud service customers (cf. PI-01).	Functional	Intersects With	Application Programming Interface (API) Security	NET-35	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	3		CLD-04
PSS-01.03B	Guidelines and Recommendations for Cloud Service Customers	The cloud service provider describes in the user documentation all necessary complementary user entity controls (CUECs) and corresponding explanations of them, so that the cloud service customer has sufficient information for appropriate risk management on its side.	Functional	Intersects With	Customer Responsibility Matrix (CRM)	CLD-03.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for security, compliance and resilience controls between the Cloud Service Provider (CSP) and its customers.	8		CLD-06.1
PSS-01.04B	Guidelines and Recommendations for Cloud Service Customers	The above-mentioned information is maintained so that it is applicable to the cloud service provided in the version intended for productive use.	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	3		TDA-04
PSS-01.01AC	Guidelines and Recommendations for Cloud Service Customers	The cloud service provider notifies cloud service customers in a timely manner about any planned modifications to the cloud service so that the affected cloud service customers can react appropriately with organisational and technical measures before the changes take effect.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		CHG-05
PSS-02.01B	Identification of Vulnerabilities of the Cloud Service	The cloud service provider applies appropriate measures to check the cloud service for vulnerabilities which might have been integrated into the cloud service during the software development process.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	5		TDA-09
PSS-02.01B	Identification of Vulnerabilities of the Cloud Service	The cloud service provider applies appropriate measures to check the cloud service for vulnerabilities which might have been integrated into the cloud service during the software development process.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	3		VPM-06
PSS-02.02B	Identification of Vulnerabilities of the Cloud Service	The procedures for identifying such vulnerabilities are part of the software development process and, depending on a risk assessment, include the following activities:	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	5		TDA-09
PSS-02.02B.1	Identification of Vulnerabilities of the Cloud Service	Static Application Security Testing;	Functional	Intersects With	Static Code Analysis	TDA-17.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	8		TDA-09.2
PSS-02.02B.2	Identification of Vulnerabilities of the Cloud Service	Dynamic Application Security Testing;	Functional	Intersects With	Dynamic Code Analysis	TDA-17.2	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	8		TDA-09.3
PSS-02.02B.3	Identification of Vulnerabilities of the Cloud Service	Code reviews by the cloud service provider's subject matter experts;	Functional	Intersects With	Manual Code Review	TDA-17.5	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ a manual code review process to identify and remediate unique flaws that require knowledge of the application's requirements and design.	8		TDA-09.7
PSS-02.02B.4	Identification of Vulnerabilities of the Cloud Service	Conducting security checks based on a list of software components or Software Bill of Materials (SBOM); and	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5		TDA-04.2
PSS-02.02B.5	Identification of Vulnerabilities of the Cloud Service	Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service.	Functional	Intersects With	Threat Intelligence Feeds	THR-04	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	3		THR-03
PSS-02.02B.5	Identification of Vulnerabilities of the Cloud Service	Obtaining information about confirmed vulnerabilities in software libraries provided by third parties and used in their own cloud service.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-06.2	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	3		VPM-04
PSS-02.03B	Identification of Vulnerabilities of the Cloud Service	The severity of identified vulnerabilities is assessed according to defined criteria and measures are taken to immediately eliminate or mitigate them.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
PSS-02.03B	Identification of Vulnerabilities of the Cloud Service	The severity of identified vulnerabilities is assessed according to defined criteria and measures are taken to immediately eliminate or mitigate them.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	3		VPM-02
PSS-02.01AC	Identification of Vulnerabilities of the Cloud Service	The procedures for identifying such vulnerabilities also include annual code reviews or security penetration tests by qualified external third parties.	Functional	Intersects With	Application Penetration Testing	TDA-17.4	Mechanisms exist to perform application-level penetration testing of custom-made Technology Assets, Applications and/or Services (TAAS).	5		TDA-09.5
PSS-02.01AC	Identification of Vulnerabilities of the Cloud Service	The procedures for identifying such vulnerabilities also include annual code reviews or security penetration tests by qualified external third parties.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-19	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5		VPM-07.1
PSS-03.01B	Informing Customers about Known Vulnerabilities	The cloud service provider ensures through a coordinated process that cloud service customers have access to regularly updated information about known vulnerabilities associated with the cloud service that may impact the information security of the customer. This includes:	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-12	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	5		THR-06
PSS-03.01B	Informing Customers about Known Vulnerabilities	The cloud service provider ensures through a coordinated process that cloud service customers have access to regularly updated information about known vulnerabilities associated with the cloud service that may impact the information security of the customer. This includes:	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	3		VPM-01
PSS-03.01B.1	Informing Customers about Known Vulnerabilities	Known-exploited vulnerabilities;	Functional	Intersects With	Known Exploited Vulnerabilities (KEV) Mitigations	VPM-06.3	Mechanisms exist to prioritize remediation and mitigation of Known Exploited Vulnerabilities (KEV) by: (1) Reducing or removing public exposure to exploitation; and	5		VPM-02.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
PSS-03.01B.2	Informing Customers about Known Vulnerabilities	Known vulnerabilities for which a patch and/or mitigating measures are provided by the cloud service provider (N-Day vulnerabilities), with appropriate references to the patch/measure; and	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	3		VPM-05
PSS-03.01B.3	Informing Customers about Known Vulnerabilities	Known vulnerabilities for which a patch and/or mitigating measures are unlikely to be provided by the cloud service provider (Forever-Day vulnerabilities), along with a justification for why they are not provided.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required	3		TDA-17
PSS-03.01B.4	Informing Customers about Known Vulnerabilities	These pertain to the provided cloud service and assets provided by the cloud service provider that the cloud service customers have to install, provide or operate within their own responsibility.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-12	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	3		THR-06
PSS-03.02B	Informing Customers about Known Vulnerabilities	The information provided to the cloud service customers includes, where available, a description of applicable and planned remediation or mitigation measures for the identified vulnerabilities.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-12	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	3		THR-06
PSS-03.02B	Informing Customers about Known Vulnerabilities	The information provided to the cloud service customers includes, where available, a description of applicable and planned remediation or mitigation measures for the identified vulnerabilities.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	3		VPM-02
PSS-03.03B	Informing Customers about Known Vulnerabilities	These vulnerabilities are also identified based on data from a list of software components or Software Bill of Materials (SBOM) data.	Functional	Intersects With	Software Bill of Materials (SBOM)	TDA-21.4	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5		TDA-04.2
PSS-03.04B	Informing Customers about Known Vulnerabilities	The vulnerabilities are presented with references to the Common Vulnerabilities and Exposures (CVE) and assessments are based on:	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
PSS-03.04B.1	Informing Customers about Known Vulnerabilities	The Common Vulnerability Scoring System (CVSS); and	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
PSS-03.04B.2	Informing Customers about Known Vulnerabilities	The Exploit Prediction Scoring System (EPSS), the Stakeholder-Specific Vulnerability Categorization (SSVC) or other similar scoring metrics	Functional	Intersects With	Vulnerability Exploitation Analysis	VPM-04	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	5		VPM-03.1
PSS-03.04B.3	Informing Customers about Known Vulnerabilities	in the latest version valid at the time of the assessment. This information is accessible to all cloud customers and supports their risk assessment and follow-up actions, with references to vulnerability-specific measures where applicable.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	3		VPM-03
PSS-03.05B	Informing Customers about Known Vulnerabilities	The cloud service provider consults the vulnerability information of its suppliers and service organisations at least daily. The published vulnerabilities are analysed in regards to their potential impact on the cloud service, and handled in accordance with the vulnerability handling process (cf. OPS-18). If the supplier or service organisation does not provide daily information, the related risk is managed according to OIS-07.	Functional	Intersects With	Threat Intelligence Feeds	THR-04	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5		THR-03
PSS-03.05B	Informing Customers about Known Vulnerabilities	The cloud service provider consults the vulnerability information of its suppliers and service organisations at least daily. The published vulnerabilities are analysed in regards to their potential impact on the cloud service, and handled in accordance with the vulnerability handling process (cf. OPS-18). If the supplier or service organisation does not provide daily information, the related risk is managed according to OIS-07.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-06.2	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	3		VPM-04
PSS-03.01AC	Informing Customers about Known Vulnerabilities	Assets provided by the cloud service provider, which must be installed, provided or operated by cloud service customers within their area of responsibility, are equipped with automatic update mechanisms. After approval by the respective cloud service customer, software updates are rolled out by the cloud service provider.	Functional	Intersects With	Alternate Sources for Continued Support	AST-39.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported Technology Assets, Applications and/or Services (TAAS).	3		TDA-17.1
PSS-03.01AC	Informing Customers about Known Vulnerabilities	Assets provided by the cloud service provider, which must be installed, provided or operated by cloud service customers within their area of responsibility, are equipped with automatic update mechanisms. After approval by the respective cloud service customer, software updates are rolled out by the cloud service provider.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	3		VPM-05
PSS-03.02AC	Informing Customers about Known Vulnerabilities	Vulnerabilities are disclosed in accordance with the Common Security Advisory Framework Version 2.0 or higher, and as specified in BSI's Technical Guideline TR-03191.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-12	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS.	3		THR-06
PSS-04.01B	Error handling and Logging Mechanisms	The cloud service provided is equipped with error handling and logging mechanisms for system components under the responsibility of the cloud service customer. These enable cloud service customers to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides.	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-07.1	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	5		CLD-06.2
PSS-04.01B	Error handling and Logging Mechanisms	The cloud service provided is equipped with error handling and logging mechanisms for system components under the responsibility of the cloud service customer. These enable cloud service customers to obtain security-related information about the security status of the cloud service as well as the data, services or functions it provides.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5		MON-03
PSS-04.02B	Error handling and Logging Mechanisms	These mechanisms are designed to address identified security risks related to the use of the cloud service. The cloud service provider identifies and documents these risks in advance, ensuring that the implemented logging mechanisms capture relevant events and activities.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	3		MON-01.8
PSS-04.02B	Error handling and Logging Mechanisms	These mechanisms are designed to address identified security risks related to the use of the cloud service. The cloud service provider identifies and documents these risks in advance, ensuring that the implemented logging mechanisms capture relevant events and activities.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
PSS-04.03B	Error handling and Logging Mechanisms	The information is detailed enough to allow cloud service customers to check the following aspects, insofar as they are applicable to the cloud service:	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-07.1	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	3		CLD-06.2
PSS-04.03B.1	Error handling and Logging Mechanisms	Which cloud service customer data and cloud service derived data, services or functions available to the cloud service customer within the cloud service, have been accessed by whom, when and from where (Audit Logs);	Functional	Intersects With	Audit Trails	MON-09.1	Mechanisms exist to link system access to individual users or service accounts.	5		MON-03.2

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
PSS-04.03B.2	Error handling and Logging Mechanisms	Malfunctions during processing of automatic or manual actions; and	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
PSS-04.03B.3	Error handling and Logging Mechanisms	Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security.	Functional	Intersects With	Control Functionality Verification	CHG-09	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	3		CHG-06
PSS-04.03B.3	Error handling and Logging Mechanisms	Changes to security-relevant configuration parameters, error handling and logging mechanisms, user authentication, action authorisation, cryptography, and communication security.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
PSS-04.04B	Error handling and Logging Mechanisms	The logged information is protected from unauthorised access and modification and can be deleted by the cloud service customer.	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
PSS-04.05B	Error handling and Logging Mechanisms	Where applicable, the cloud service customer can activate or de-activate the logging and can control the scope and verbosity of the logging the cloud service provides.	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	3		MON-03
PSS-04.06B	Error handling and Logging Mechanisms	The logging of management plane actions by the cloud service customers covers all relevant systems and system components.	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-07.1	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	3		CLD-06.2
PSS-04.06B	Error handling and Logging Mechanisms	The logging of management plane actions by the cloud service customers covers all relevant systems and system components.	Functional	Intersects With	Audit Trails	MON-09.1	Mechanisms exist to link system access to individual users or service accounts.	3		MON-03.2
PSS-04.01AC	Error handling and Logging Mechanisms	Cloud service customers can retrieve security-related information via documented interfaces which are suitable for further processing this information as part of their Security Information and Event Management (SIEM).	Functional	Intersects With	Multi-Tenant Event Logging Capabilities	CLD-07.1	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.	5		CLD-06.2
PSS-04.01AC	Error handling and Logging Mechanisms	Cloud service customers can retrieve security-related information via documented interfaces which are suitable for further processing this information as part of their Security Information and Event Management (SIEM).	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry.	3		MON-02
PSS-05.01B	Authentication Mechanisms	The cloud service provided is equipped with authentication mechanisms that can force multi-factor authentication for users, IT components or applications within the cloud service customers' area of responsibility. These authentication mechanisms are set up at all access points that allow users, IT components or applications to interact with the cloud service.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
PSS-05.02B	Authentication Mechanisms	For privileged users, IT components or applications under the responsibility of the cloud service customer, these authentication mechanisms can be enforced by the cloud service customer.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	3		IAC-16
PSS-05.02B	Authentication Mechanisms	For privileged users, IT components or applications under the responsibility of the cloud service customer, these authentication mechanisms can be enforced by the cloud service customer.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
PSS-05.01AC	Authentication Mechanisms	The cloud service offers out-of-band (OOB) authentication, in which the factors are transmitted via different channels (e.g. Internet and mobile network).	Functional	Intersects With	Out-of-Band (OOB) Multi-Factor Authentication (MFA)	IAC-37.3	Mechanisms exist to implement Out-of-Band (OOB) Multi-Factor Authentication (MFA) for access to privileged and non-privileged accounts such that one of the factors is independently provided by a device separate from the system being accessed.	8		IAC-06.4
PSS-06.01B	Session Management	To protect confidentiality, availability, integrity and authenticity during interactions with the cloud service, a suitable session management system is used that corresponds to the established rules of technology and is protected against known attacks.	Functional	Intersects With	Session Integrity	NET-29	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5		NET-09
PSS-06.01B	Session Management	To protect confidentiality, availability, integrity and authenticity during interactions with the cloud service, a suitable session management system is used that corresponds to the established rules of technology and is protected against known attacks.	Functional	Intersects With	Client-Facing Web Services	WEB-06	Mechanisms exist to deploy reasonably-expected security, compliance and resilience controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	3		WEB-04
PSS-06.02B	Session Management	Mechanisms are implemented that invalidate a session after it has been detected as inactive. The inactivity can be detected by time measurement. In this case, the time interval can be configured by the cloud service provider or - if technically possible - by the cloud service customer.	Functional	Intersects With	Session Lock	CFG-04.3	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	3		IAC-24
PSS-06.02B	Session Management	Mechanisms are implemented that invalidate a session after it has been detected as inactive. The inactivity can be detected by time measurement. In this case, the time interval can be configured by the cloud service provider or - if technically possible - by the cloud service customer.	Functional	Intersects With	Session Termination	CFG-04.5	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	8		IAC-25
PSS-07.01B	Confidentiality of Authentication Information	If passwords are used as authentication information for the cloud service, the cloud service provider provides the cloud service customers with the following procedures to protect the confidentiality of the passwords:	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
PSS-07.01B.1	Confidentiality of Authentication Information	Users can initially create the password themselves or must change an initial password when logging in to the cloud service for the first time. An initial password loses its validity after a maximum of 14 days;	Functional	Intersects With	Default Authenticators	IAC-14.4	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5		IAC-10.8
PSS-07.01B.2	Confidentiality of Authentication Information	When creating passwords, compliance with the length and complexity requirements of the cloud service provider (cf. IAM-08) or the cloud service customer is technically enforced;	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
PSS-07.01B.3	Confidentiality of Authentication Information	The user is informed about changing or resetting the password. Password reset procedures are valid for at most 48 hours. After the reset procedure has been used, the password is to be changed by the user; and	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	3		IAC-10
PSS-07.01B.4	Confidentiality of Authentication Information	The server-side storage uses hash functions in combination with salt values, both corresponding to the state of the art.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: **Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)**
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
PSS-07.02B	Confidentiality of Authentication Information	Rules and recommendations are shared with the cloud service customers as applicable to the users under their responsibility. The cloud service provider offers the cloud service customers tools for the management and enforcement of these rules.	Functional	Intersects With	User Responsibilities for Account Management	IAC-22	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards and	5		IAC-18
PSS-07.03B	Confidentiality of Authentication Information	When distributing credentials, the cloud service provider verifies the recipient's identity, validates the request and protects the credentials by using additional security mechanisms such as multi-factor authentication.	Functional	Intersects With	Identity Proofing (Identity Verification)	IAC-05	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	3		IAC-28
PSS-07.03B	Confidentiality of Authentication Information	When distributing credentials, the cloud service provider verifies the recipient's identity, validates the request and protects the credentials by using additional security mechanisms such as multi-factor authentication.	Functional	Intersects With	Authenticator Management	IAC-14	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5		IAC-10
PSS-08.01B	Roles and Rights Framework	The cloud service provided comprises a roles and rights framework for users of the cloud service customer. This framework allows users to manage their own access rights. It describes access rights and roles for the functions provided by the cloud service. Cloud service customers can configure relevant access control parameters themselves.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5		IAC-08
PSS-08.02B	Roles and Rights Framework	The access rights and roles are suitable for enabling users of the cloud service customer to manage access authorisations and permissions in accordance with the principle of least-privilege and how it is necessary for the performance of tasks ('need-to-know-principle') and to implement the principle of functional separation between operational and controlling functions ('segregation of duties').	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	3		HRS-11
PSS-08.02B	Roles and Rights Framework	The access rights and roles are suitable for enabling users of the cloud service customer to manage access authorisations and permissions in accordance with the principle of least-privilege and how it is necessary for the performance of tasks ('need-to-know-principle') and to implement the principle of functional separation between operational and controlling functions ('segregation of duties').	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5		IAC-21
PSS-08.03B	Roles and Rights Framework	The cloud service provided is equipped with a functionality to help cloud service customers review user access rights under their responsibility.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	5		IAC-17
PSS-08.04B	Roles and Rights Framework	In case the cloud service includes the management of customer identities, for a given customer identity, the cloud service provided is equipped with a functionality to provide the list of access rights currently granted to that identity according to the contractual terms.	Functional	Intersects With	User & Service Account Inventories	IAC-08.3	Mechanisms exist to maintain a current list of authorized users and service accounts.	3		IAC-01.3
PSS-08.04B	Roles and Rights Framework	In case the cloud service includes the management of customer identities, for a given customer identity, the cloud service provided is equipped with a functionality to provide the list of access rights currently granted to that identity according to the contractual terms.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	3		IAC-17
PSS-09.01B	Authorisation Mechanisms	Access to the functions provided by the cloud service is restricted by access controls (authorisation mechanisms) that verify whether users, IT components, or applications are authorised to perform certain actions.	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	8		IAC-20
PSS-09.02B	Authorisation Mechanisms	The cloud service provider validates the functionality of the authorisation mechanisms before new functions are made available to cloud service customers and in the event of changes to the authorisation mechanisms of existing functions (cf. DEV-07).	Functional	Intersects With	Control Functionality Verification	CHG-09	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5		CHG-06
PSS-09.02B	Authorisation Mechanisms	The cloud service provider validates the functionality of the authorisation mechanisms before new functions are made available to cloud service customers and in the event of changes to the authorisation mechanisms of existing functions (cf. DEV-07).	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	3		TDA-09
PSS-09.03B	Authorisation Mechanisms	If validation activities reveal vulnerabilities, the procedures for identifying vulnerabilities (cf. PSS-02) are applied and measures for timely remediation or mitigation are initiated.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
PSS-09.01AC	Authorisation Mechanisms	Access controls are attribute-based to enable granular and contextual checks against multiple attributes of a user, IT component, or application (e.g., role, location, authentication method).	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-06	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	3		IAC-08
PSS-09.01AC	Authorisation Mechanisms	Access controls are attribute-based to enable granular and contextual checks against multiple attributes of a user, IT component, or application (e.g., role, location, authentication method).	Functional	Intersects With	Adaptive Identification & Authentication	IAC-41	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.	3		IAC-13
PSS-10.01B	Software Defined Networking	If the cloud service offers functions for software-defined networking (SDN), the confidentiality of cloud service customer data is ensured by suitable SDN procedures.	Functional	Intersects With	Multi-Tenant Environments	CLD-07	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	3		CLD-06
PSS-10.01B	Software Defined Networking	If the cloud service offers functions for software-defined networking (SDN), the confidentiality of cloud service customer data is ensured by suitable SDN procedures.	Functional	Intersects With	Software Defined Networking (SDN)	NET-12	Automated mechanisms exist to enable dynamic, policy-driven network segmentation, access controls and traffic management with a Software Defined Networking (SDN) architecture.	5		NET-06.7
PSS-10.02B	Software Defined Networking	The cloud service provider validates the functionality of the SDN functions before providing new SDN features to cloud service customers or modifying existing SDN features. Identified defects are assessed and corrected in a risk-oriented manner.	Functional	Intersects With	Control Functionality Verification	CHG-09	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	3		CHG-06
PSS-10.02B	Software Defined Networking	The cloud service provider validates the functionality of the SDN functions before providing new SDN features to cloud service customers or modifying existing SDN features. Identified defects are assessed and corrected in a risk-oriented manner.	Functional	Intersects With	Software Defined Networking (SDN)	NET-12	Automated mechanisms exist to enable dynamic, policy-driven network segmentation, access controls and traffic management with a Software Defined Networking (SDN) architecture.	3		NET-06.7
PSS-11.01B	Images for Virtual Machines and Containers	If cloud service customers operate virtual machines or containers with the cloud service, the cloud service provided is equipped with functionalities that ensure the following aspects:	Functional	Intersects With	Virtual Machine Images	SEA-23.1	Mechanisms exist to ensure the integrity of virtual machine images at all times.	5		CLD-05
PSS-11.01B	Images for Virtual Machines and Containers	If cloud service customers operate virtual machines or containers with the cloud service, the cloud service provided is equipped with functionalities that ensure the following aspects:	Functional	Intersects With	Application Container	SEA-31	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	3		SEA-21
PSS-11.01B.1	Images for Virtual Machines and Containers	Cloud service customers can restrict the selection of images of virtual machines or containers according to their specifications, so that users of the cloud service customer can only launch the images or containers released according to these restrictions;	Functional	Intersects With	Restrict Roles Permitted To Install Software	CFG-12	Automated mechanisms exist to prevent the installation of software, unless the action is performed by a privileged user or service.	3		CFG-05
PSS-11.01B.1	Images for Virtual Machines and Containers	Cloud service customers can restrict the selection of images of virtual machines or containers according to their specifications, so that users of the cloud service customer can only launch the images or containers released according to these restrictions;	Functional	Intersects With	Virtual Machine Images	SEA-23.1	Mechanisms exist to ensure the integrity of virtual machine images at all times.	3		CLD-05
PSS-11.01B.2	Images for Virtual Machines and Containers	If the cloud service provider provides images of virtual machines or containers to the cloud service customer, the cloud service provider appropriately informs the cloud service customer of the changes made to the previous version;	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	3		CHG-05
PSS-11.01B.3	Images for Virtual Machines and Containers	Images provided by the cloud service provider are labelled with information regarding their origin; and	Functional	Intersects With	Provenance	AST-14	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	3		AST-03.2
PSS-11.01B.3	Images for Virtual Machines and Containers	Images provided by the cloud service provider are labelled with information regarding their origin; and	Functional	Intersects With	Virtual Machine Images	SEA-23.1	Mechanisms exist to ensure the integrity of virtual machine images at all times.	3		CLD-05
PSS-11.01B.4	Images for Virtual Machines and Containers	Images provided by the cloud service provider are hardened according to generally accepted industry standards.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Germany - Cloud Computing Compliance Controls Catalogue (C5) (2026)
Focal Document URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2026/C5_2026.pdf?__blob=publicationFil
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-deu-c5-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
PSS-11.01B.4	Images for Virtual Machines and Containers	Images provided by the cloud service provider are hardened according to generally accepted industry standards.	Functional	Intersects With	Virtual Machine Images	SEA-23.1	Mechanisms exist to ensure the integrity of virtual machine images at all times.	3		CLD-05
PSS-11.01AC	Images for Virtual Machines and Containers	The cloud service provider checks the integrity and authenticity of virtual machines or container images at startup and informs the cloud service customer accordingly about the results of those checks.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-11	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	3		END-06
PSS-11.01AC	Images for Virtual Machines and Containers	The cloud service provider checks the integrity and authenticity of virtual machines or container images at startup and informs the cloud service customer accordingly about the results of those checks.	Functional	Intersects With	Software / Firmware Integrity Verification	TDA-20.3	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	5		TDA-14.1
PSS-11.02AC	Images for Virtual Machines and Containers	During runtime, the cloud service provider protects the virtual machines or container images against tampering and informs the cloud service customer accordingly about the status during runtime.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-11	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	3		END-06
PSS-11.02AC	Images for Virtual Machines and Containers	During runtime, the cloud service provider protects the virtual machines or container images against tampering and informs the cloud service customer accordingly about the status during runtime.	Functional	Intersects With	Application Container	SEA-31	Mechanisms exist to utilize an application container (virtualization approach) to isolate to a known set of dependencies, access methods and interfaces.	3		SEA-21
PSS-12.01B	Region of Data Processing and Storage	The architecture of the cloud service, including the technical design of its infrastructure, ensures that cloud service customer data and eventual data backups thereof are processed and stored only in the region specified in the contractual agreements with the cloud service provider. If the cloud service customer is able to select from multiple regions, processing and storage of the aforementioned data is limited to the selected regions.	Functional	Intersects With	Geographic Data Location	DCH-30	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within geographically distributed Technology Assets, Applications and/or Services (TAAS) (physical and virtual).	3		DCH-19
PSS-12.01B	Region of Data Processing and Storage	The architecture of the cloud service, including the technical design of its infrastructure, ensures that cloud service customer data and eventual data backups thereof are processed and stored only in the region specified in the contractual agreements with the cloud service provider. If the cloud service customer is able to select from multiple regions, processing and storage of the aforementioned data is limited to the selected regions.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	8		CLD-09
PSS-12.02B	Region of Data Processing and Storage	Processing and storage of cloud service customer data within the service organisations of the cloud service provider also adheres to the regions selected by the cloud service customer.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	3		CLD-09
PSS-12.02B	Region of Data Processing and Storage	Processing and storage of cloud service customer data within the service organisations of the cloud service provider also adheres to the regions selected by the cloud service customer.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
PSS-12.03B	Region of Data Processing and Storage	The contractual agreements specify the regions in which processing and storage of cloud service customer data, cloud service derived data and account data occurs and the circumstances under which changes may be applied.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	5		CLD-09
PSS-12.03B	Region of Data Processing and Storage	The contractual agreements specify the regions in which processing and storage of cloud service customer data, cloud service derived data and account data occurs and the circumstances under which changes may be applied.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	3		TPM-05
PSS-12.04B	Region of Data Processing and Storage	Customers are notified beforehand in case of any changes to the regions in which the aforementioned data is processed or stored. If the cloud service provider has not been granted prior general authorisation by the cloud service customer to do so, such authorisations are obtained in accordance with the requirements specified in the contractual agreements or let the cloud service customer exercise termination rights.	Functional	Intersects With	Stakeholder Notification of Changes	CHG-08	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5		CHG-05
PSS-12.04B	Region of Data Processing and Storage	Customers are notified beforehand in case of any changes to the regions in which the aforementioned data is processed or stored. If the cloud service provider has not been granted prior general authorisation by the cloud service customer to do so, such authorisations are obtained in accordance with the requirements specified in the contractual agreements or let the cloud service customer exercise termination rights.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	3		CLD-09
PSS-12.01AS	Region of Data Processing and Storage	PSS-12.01AS, sharpening PSS-12.01B The architecture of the cloud service, including the technical design of its infrastructure, ensures that the cloud service customer data, cloud service derived data and eventual data backups thereof are processed and stored only in the region specified in the contractual agreements with the cloud service provider. If the cloud service customer is able to select from multiple regions, processing and storage of the aforementioned data is limited to the selected regions.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	8		CLD-09
PSS-12.02AS	Region of Data Processing and Storage	PSS-12.02AS, sharpening PSS-12.02B Processing and storage of cloud service customer data and cloud service derived data within the service organisations of the cloud service provider also adheres to the regions selected by the cloud service customer.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
PSS-12.01AC	Region of Data Processing and Storage	The cloud service provider offers partitions selectable by the cloud service customer where partition-specific identity management is enforced for both cloud service customers and all cloud service provider personnel. Identity verification and identity storage are confined to the geographical boundaries of the selected partition.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	3		CLD-09
PSS-12.01AC	Region of Data Processing and Storage	The cloud service provider offers partitions selectable by the cloud service customer where partition-specific identity management is enforced for both cloud service customers and all cloud service provider personnel. Identity verification and identity storage are confined to the geographical boundaries of the selected partition.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	3		IAC-01
PSS-12.02AC	Region of Data Processing and Storage	Within these partitions, the following operations by the cloud service provider are restricted to occur only within the geographical boundaries of the customer-selected partitions:	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	3		CLD-09
PSS-12.02AC.1	Region of Data Processing and Storage	Privileged access to the production environment by the cloud service provider, including potential access to cloud service customer data and cloud service derived data;	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	3		CLD-09
PSS-12.02AC.1	Region of Data Processing and Storage	Privileged access to the production environment by the cloud service provider, including potential access to cloud service customer data and cloud service derived data;	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	3		IAC-16
PSS-12.02AC.2	Region of Data Processing and Storage	System logging and event monitoring by the cloud service provider, except for processing event logs specifically for threat intelligence and handling IP addresses for routing purposes; and	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	3		CLD-09
PSS-12.02AC.2	Region of Data Processing and Storage	System logging and event monitoring by the cloud service provider, except for processing event logs specifically for threat intelligence and handling IP addresses for routing purposes; and	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
PSS-12.02AC.3	Region of Data Processing and Storage	Cryptographic key management and storage practices to ensure keys are handled and stored within limits of the partition.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	3		CRY-09
PSS-12.02AC.3	Region of Data Processing and Storage	Cryptographic key management and storage practices to ensure keys are handled and stored within limits of the partition.	Functional	Intersects With	Geolocation Requirements for Processing, Storage and Service Locations	DCH-30.1	Mechanisms exist to control the location of Technology Assets, Applications and/or Services (TAAS) processing and/or storage based on business requirements that includes statutory, regulatory and contractual obligations.	3		CLD-09
PSS-12.02AC.4	Region of Data Processing and Storage	These restrictions considering partitions also apply to any service organisations involved in the operation of the cloud service.	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	3		TPM-04.4