NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **Trusted Information Security Assessment Exchange (TISAX) 6.0.3**
Focal Document URL: https://portal.enx.com/en-US/TISAX/downloads/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-tisax-6-0-3.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
1	IS Policies and Organization	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.1	Information Security Policies	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.1.1	N/A	+ The requirements for information security have been determined and documented: - The requirements are adapted to the organization's goals, - A policy is prepared and is released by the organization. + The policy includes objectives and the significance of information security within the organization.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
1.1.1	N/A	+ The requirements for information security have been determined and documented: - The requirements are adapted to the organization's goals, - A policy is prepared and is released by the organization. + The policy includes objectives and the significance of information security within the organization.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
1.1.1	N/A	+ The requirements for information security have been determined and documented: - The requirements are adapted to the organization's goals, - A policy is prepared and is released by the organization. + The policy includes objectives and the significance of information security within the organization.	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal security, compliance and resilience control system.	5	
1.1.1	N/A	+ The requirements for information security have been determined and documented: - The requirements are adapted to the organization's goals, - A policy is prepared and is released by the organization. + The policy includes objectives and the significance of information security within the organization.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
1.2	Organization of Information Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.2.1	N/A	+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). + Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed ISA catalogue). + The effectiveness of the ISMS is regularly reviewed by the management.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
1.2.1	N/A	+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). + Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed ISA catalogue). + The effectiveness of the ISMS is regularly reviewed by the management.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
1.2.1	N/A	+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). + Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed ISA catalogue). + The effectiveness of the ISMS is regularly reviewed by the management.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	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	
1.2.1	N/A	+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). + Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed ISA catalogue). + The effectiveness of the ISMS is regularly reviewed by the management.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
1.2.1	N/A	+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). + Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed ISA catalogue). + The effectiveness of the ISMS is regularly reviewed by the management.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
1.2.1	N/A	+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). + Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed ISA catalogue). + The effectiveness of the ISMS is regularly reviewed by the management.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
1.2.1	N/A	+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). + Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed ISA catalogue). + The effectiveness of the ISMS is regularly reviewed by the management.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
1.2.1	N/A	+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). + Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed ISA catalogue). + The effectiveness of the ISMS is regularly reviewed by the management.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
1.2.1	N/A	+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). + Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed ISA catalogue). + The effectiveness of the ISMS is regularly reviewed by the management.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
1.2.1	N/A	+ The scope of the ISMS (the organization managed by the ISMS) is defined. + The organization's requirements for the ISMS are determined. + The organizational management has commissioned and approved the ISMS. + The ISMS provides the organizational management with suitable monitoring and control means (e.g. management review). + Applicable controls have been determined (e.g. ISO 27001 Statement of Applicability, completed ISA catalogue). + The effectiveness of the ISMS is regularly reviewed by the management.	Functional	Intersects With	Compliance Scope	CPL-01.2	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	
1.2.2	N/A	+ Responsibilities for information security within the organization are defined, documented, and assigned. + The responsible employees are defined and qualified for their task. + The required resources are available. + The contact persons are known within the organization and to relevant business partners.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	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	
1.2.2	N/A	+ Responsibilities for information security within the organization are defined, documented, and assigned. + The responsible employees are defined and qualified for their task. + The required resources are available. + The contact persons are known within the organization and to relevant business partners.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
1.2.2	N/A	+ Responsibilities for information security within the organization are defined, documented, and assigned. + The responsible employees are defined and qualified for their task. + The required resources are available. + The contact persons are known within the organization and to relevant business partners.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
1.2.2	N/A	+ Responsibilities for information security within the organization are defined, documented, and assigned. + The responsible employees are defined and qualified for their task. + The required resources are available. + The contact persons are known within the organization and to relevant business partners.	Functional	Intersects With	Position Categorization	HRS-02	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	
1.2.2	N/A	+ Responsibilities for information security within the organization are defined, documented, and assigned. + The responsible employees are defined and qualified for their task. + The required resources are available. + The contact persons are known within the organization and to relevant business partners.	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
1.2.2	N/A	+ Responsibilities for information security within the organization are defined, documented, and assigned. + The responsible employees are defined and qualified for their task. + The required resources are available. + The contact persons are known within the organization and to relevant business partners.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
1.2.2	N/A	+ Responsibilities for information security within the organization are defined, documented, and assigned. + The responsible employees are defined and qualified for their task. + The required resources are available. + The contact persons are known within the organization and to relevant business partners.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
1.2.3	N/A	+ Projects are classified while taking into account the information security requirements.	Functional	Intersects With	Asset Scope Classification	AST-04.1	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).	5	
1.2.3	N/A	+ Projects are classified while taking into account the information security requirements.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
1.2.3	N/A	+ Projects are classified while taking into account the information security requirements.	Functional	Subset Of	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	10	
1.2.3	N/A	+ Projects are classified while taking into account the information security requirements.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
1.2.4	N/A	+ The concerned services and IT services used are identified. + The security requirements relevant to the IT service are determined: + The organization responsible for implementing the requirement is defined and aware of its responsibility. + Mechanisms for shared responsibilities are specified and implemented. + The responsible organization fulfils its respective responsibilities.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	

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
1.2.4	N/A	+ The concerned services and IT services used are identified. + The security requirements relevant to the IT service are determined: + The organization responsible for implementing the requirement is defined and aware of its responsibility. + Mechanisms for shared responsibilities are specified and implemented. + The responsible organization fulfils its respective responsibilities.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
1.2.4	N/A	+ The concerned services and IT services used are identified. + The security requirements relevant to the IT service are determined: + The organization responsible for implementing the requirement is defined and aware of its responsibility. + Mechanisms for shared responsibilities are specified and implemented. + The responsible organization fulfils its respective responsibilities.	Functional	Intersects With	Asset Scope Classification	AST-04.1	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).	5	
1.2.4	N/A	+ The concerned services and IT services used are identified. + The security requirements relevant to the IT service are determined: + The organization responsible for implementing the requirement is defined and aware of its responsibility. + Mechanisms for shared responsibilities are specified and implemented. + The responsible organization fulfils its respective responsibilities.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
1.2.4	N/A	+ The concerned services and IT services used are identified. + The security requirements relevant to the IT service are determined: + The organization responsible for implementing the requirement is defined and aware of its responsibility. + Mechanisms for shared responsibilities are specified and implemented. + The responsible organization fulfils its respective responsibilities.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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).	5	
1.2.4	N/A	+ The concerned services and IT services used are identified. + The security requirements relevant to the IT service are determined: + The organization responsible for implementing the requirement is defined and aware of its responsibility. + Mechanisms for shared responsibilities are specified and implemented. + The responsible organization fulfils its respective responsibilities.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	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	
1.3	Asset Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.3.1	N/A	+ Information assets and other assets where security is relevant to the organization are identified and recorded. · A person responsible for these information assets is assigned. + The supporting assets processing the information assets are identified and recorded: · A person responsible for these supporting assets is assigned.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
1.3.1	N/A	+ Information assets and other assets where security is relevant to the organization are identified and recorded. · A person responsible for these information assets is assigned. + The supporting assets processing the information assets are identified and recorded: · A person responsible for these supporting assets is assigned.	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
1.3.1	N/A	+ Information assets and other assets where security is relevant to the organization are identified and recorded. · A person responsible for these information assets is assigned. + The supporting assets processing the information assets are identified and recorded: · A person responsible for these supporting assets is assigned.	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset 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.	5	
1.3.2	N/A	+ A consistent scheme for the classification of information assets regarding the protection goal of confidentiality is available. + Evaluation of the identified information assets is carried out according to the defined criteria and assigned to the existing classification scheme. + Specifications for the handling of supporting assets (e.g. identification, correct handling, transport, storage, return, deletion/disposal) depending on the classification of information assets are in place and implemented.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	
1.3.2	N/A	+ A consistent scheme for the classification of information assets regarding the protection goal of confidentiality is available. + Evaluation of the identified information assets is carried out according to the defined criteria and assigned to the existing classification scheme. + Specifications for the handling of supporting assets (e.g. identification, correct handling, transport, storage, return, deletion/disposal) depending on the classification of information assets are in place and implemented.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	5	
1.3.2	N/A	+ A consistent scheme for the classification of information assets regarding the protection goal of confidentiality is available. + Evaluation of the identified information assets is carried out according to the defined criteria and assigned to the existing classification scheme. + Specifications for the handling of supporting assets (e.g. identification, correct handling, transport, storage, return, deletion/disposal) depending on the classification of information assets are in place and implemented.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
1.3.3	N/A	+ External IT services are not used without explicit assessment and implementation of the information security requirements: · A risk assessment of the external IT services is available, · Legal, regulatory, and contractual requirements are considered. + The external IT services have been harmonized with the protection need of the processed information assets.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
1.3.3	N/A	+ External IT services are not used without explicit assessment and implementation of the information security requirements: · A risk assessment of the external IT services is available, · Legal, regulatory, and contractual requirements are considered. + The external IT services have been harmonized with the protection need of the processed information assets.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
1.3.3	N/A	+ External IT services are not used without explicit assessment and implementation of the information security requirements: · A risk assessment of the external IT services is available, · Legal, regulatory, and contractual requirements are considered. + The external IT services have been harmonized with the protection need of the processed information assets.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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).	5	
1.3.3	N/A	+ External IT services are not used without explicit assessment and implementation of the information security requirements: · A risk assessment of the external IT services is available, · Legal, regulatory, and contractual requirements are considered. + The external IT services have been harmonized with the protection need of the processed information assets.	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	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	
1.3.4	N/A	+ Software is approved before installation or use. The following aspects are considered: · Limited approval for specific use-cases or roles · Conformance to the information security requirements · Software use rights and licensing · Source / reputation of the software + Software approval also applies to special purpose software such as maintenance tools	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5	
1.3.4	N/A	+ Software is approved before installation or use. The following aspects are considered: · Limited approval for specific use-cases or roles · Conformance to the information security requirements · Software use rights and licensing · Source / reputation of the software + Software approval also applies to special purpose software such as maintenance tools	Functional	Intersects With	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	5	
1.3.4	N/A	+ Software is approved before installation or use. The following aspects are considered: · Limited approval for specific use-cases or roles · Conformance to the information security requirements · Software use rights and licensing · Source / reputation of the software + Software approval also applies to special purpose software such as maintenance tools	Functional	Intersects With	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.	5	
1.3.4	N/A	+ Software is approved before installation or use. The following aspects are considered: · Limited approval for specific use-cases or roles · Conformance to the information security requirements · Software use rights and licensing · Source / reputation of the software + Software approval also applies to special purpose software such as maintenance tools	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
1.4	IS Risk Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.4.1	N/A	+ Risk assessments are carried out both at regular intervals and in response to events. + Information security risks are appropriately assessed (e.g. for probability of occurrence and potential damage). + Information security risks are documented. + A responsible person (risk owner) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
1.4.1	N/A	+ Risk assessments are carried out both at regular intervals and in response to events. + Information security risks are appropriately assessed (e.g. for probability of occurrence and potential damage). + Information security risks are documented. + A responsible person (risk owner) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.	Functional	Intersects With	Risk Framing	RSK-01.1	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.	5	
1.4.1	N/A	+ Risk assessments are carried out both at regular intervals and in response to events. + Information security risks are appropriately assessed (e.g. for probability of occurrence and potential damage). + Information security risks are documented. + A responsible person (risk owner) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
1.4.1	N/A	+ Risk assessments are carried out both at regular intervals and in response to events. + Information security risks are appropriately assessed (e.g. for probability of occurrence and potential damage). + Information security risks are documented. + A responsible person (risk owner) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.	Functional	Intersects With	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
1.4.1	N/A	+ Risk assessments are carried out both at regular intervals and in response to events. + Information security risks are appropriately assessed (e.g. for probability of occurrence and potential damage). + Information security risks are documented. + A responsible person (risk owner) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.	Functional	Intersects With	Risk Assessment	RSK-04	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	
1.4.1	N/A	+ Risk assessments are carried out both at regular intervals and in response to events. + Information security risks are appropriately assessed (e.g. for probability of occurrence and potential damage). + Information security risks are documented. + A responsible person (risk owner) is assigned to each information security risk. This person is responsible for the assessment and handling of the information security risks.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
1.5	Assessments	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

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
1.5.1	N/A	+ Observation of policies is verified throughout the organization. + Information security policies and procedures are reviewed at regular intervals. + Measures for correcting potential non-conformities (deviations) are initiated and pursued. + Compliance with information security requirements (e.g. technical specifications) is verified at regular intervals. + The results of the conducted reviews are recorded and retained.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
1.5.1	N/A	+ Observation of policies is verified throughout the organization. + Information security policies and procedures are reviewed at regular intervals. + Measures for correcting potential non-conformities (deviations) are initiated and pursued. + Compliance with information security requirements (e.g. technical specifications) is verified at regular intervals. + The results of the conducted reviews are recorded and retained.	Functional	Intersects With	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
1.5.1	N/A	+ Observation of policies is verified throughout the organization. + Information security policies and procedures are reviewed at regular intervals. + Measures for correcting potential non-conformities (deviations) are initiated and pursued. + Compliance with information security requirements (e.g. technical specifications) is verified at regular intervals. + The results of the conducted reviews are recorded and retained.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	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.	5	
1.5.1	N/A	+ Observation of policies is verified throughout the organization. + Information security policies and procedures are reviewed at regular intervals. + Measures for correcting potential non-conformities (deviations) are initiated and pursued. + Compliance with information security requirements (e.g. technical specifications) is verified at regular intervals. + The results of the conducted reviews are recorded and retained.	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
1.5.1	N/A	+ Observation of policies is verified throughout the organization. + Information security policies and procedures are reviewed at regular intervals. + Measures for correcting potential non-conformities (deviations) are initiated and pursued. + Compliance with information security requirements (e.g. technical specifications) is verified at regular intervals. + The results of the conducted reviews are recorded and retained.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
1.5.1	N/A	+ Observation of policies is verified throughout the organization. + Information security policies and procedures are reviewed at regular intervals. + Measures for correcting potential non-conformities (deviations) are initiated and pursued. + Compliance with information security requirements (e.g. technical specifications) is verified at regular intervals. + The results of the conducted reviews are recorded and retained.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
1.5.2	N/A	+ Information security reviews are carried out by an independent and competent body at regular intervals and in case of fundamental changes. + Measures for correcting potential deviations are initiated and pursued.	Functional	Equal	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	10	
1.5.2	N/A	+ Information security reviews are carried out by an independent and competent body at regular intervals and in case of fundamental changes. + Measures for correcting potential deviations are initiated and pursued.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	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	
1.5.2	N/A	+ Information security reviews are carried out by an independent and competent body at regular intervals and in case of fundamental changes. + Measures for correcting potential deviations are initiated and pursued.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-05	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	5	
1.6	Incident and Crisis Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
1.6.1	N/A	+ A definition for a reportable security event or observation exists and is known by employees and relevant stakeholders. The following aspects are considered: - Events and observations related to personnel (e.g., misconduct / misbehaviour) - Events and observations related to physical security (e.g., intrusion, theft, unauthorized access to security zones, vulnerabilities in the security zones) - Events and observations related to IT and cyber security (e.g., vulnerable IT-systems, detected successful or unsuccessful attacks) - Events and observations related to suppliers and other business partners (e.g., any incidents that can have negative effect on the security of own organization) + Adequate mechanisms based on perceived risks to report security events are defined, implemented, and known to all relevant potential reporters + Adequate channels for communication with event reporters exist.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
1.6.1	N/A	+ A definition for a reportable security event or observation exists and is known by employees and relevant stakeholders. The following aspects are considered: - Events and observations related to personnel (e.g., misconduct / misbehaviour) - Events and observations related to physical security (e.g., intrusion, theft, unauthorized access to security zones, vulnerabilities in the security zones) - Events and observations related to IT and cyber security (e.g., vulnerable IT-systems, detected successful or unsuccessful attacks) - Events and observations related to suppliers and other business partners (e.g., any incidents that can have negative effect on the security of own organization) + Adequate mechanisms based on perceived risks to report security events are defined, implemented, and known to all relevant potential reporters + Adequate channels for communication with event reporters exist.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5	
1.6.2	N/A	+ Reported events are processed without undue delay. + An adequate reaction to reported security events is ensured. + Lessons learned are incorporated into continuous improvement.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
1.6.2	N/A	+ Reported events are processed without undue delay. + An adequate reaction to reported security events is misured. + Lessons learned are incorporated into continuous improvement.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	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	
1.6.2	N/A	+ Reported events are processed without undue delay. + An adequate reaction to reported security events is ensured. + Lessons learned are incorporated into continuous improvement.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable:(1) Internal stakeholders;(2) Affected clients & third-parties; and(3) Regulatory authorities.	5	
1.6.2	N/A	+ Reported events are processed without undue delay. + An adequate reaction to reported security events is misured. + Lessons learned are incorporated into continuous improvement.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	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	
1.6.3	N/A	+ An appropriate planning to react to and recover from crisis situations exists. - The required resources are available. + Responsibilities and authority for crisis management within the organization are defined, documented, and assigned. + The responsible employees are defined and qualified for their task.	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
1.6.3	N/A	+ An appropriate planning to react to and recover from crisis situations exists. - The required resources are available. + Responsibilities and authority for crisis management within the organization are defined, documented, and assigned. + The responsible employees are defined and qualified for their task.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
1.6.3	N/A	+ An appropriate planning to react to and recover from crisis situations exists. - The required resources are available. + Responsibilities and authority for crisis management within the organization are defined, documented, and assigned. + The responsible employees are defined and qualified for their task.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	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.	5	
2	Human Resources	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2.1.1	N/A	+ Sensitive work fields and jobs are determined. + The requirements for employees with respect to their job profiles are determined and fulfilled. + The identity of potential employees is verified (e.g. checking identity documents).	Functional	Intersects With	Position Categorization	HRS-02	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	
2.1.1	N/A	+ Sensitive work fields and jobs are determined. + The requirements for employees with respect to their job profiles are determined and fulfilled. + The identity of potential employees is verified (e.g. checking identity documents).	Functional	Intersects With	Users With Elevated Privileges	HRS-02.1	Mechanisms exist to ensure that every user accessing Technology Assets, Applications and/or Services (TAAS) that process, store and/or transmit sensitive/regulated data is cleared and regularly trained to handle the information in question.	5	
2.1.1	N/A	+ Sensitive work fields and jobs are determined. + The requirements for employees with respect to their job profiles are determined and fulfilled. + The identity of potential employees is verified (e.g. checking identity documents).	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
2.1.1	N/A	+ Sensitive work fields and jobs are determined. + The requirements for employees with respect to their job profiles are determined and fulfilled. + The identity of potential employees is verified (e.g. checking identity documents).	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
2.1.1	N/A	+ Sensitive work fields and jobs are determined. + The requirements for employees with respect to their job profiles are determined and fulfilled. + The identity of potential employees is verified (e.g. checking identity documents).	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
2.1.1	N/A	+ Sensitive work fields and jobs are determined. + The requirements for employees with respect to their job profiles are determined and fulfilled. + The identity of potential employees is verified (e.g. checking identity documents).	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	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	
2.1.2	N/A	+ A non-disclosure obligation is in effect. + An obligation to comply with the information security policies is in effect.	Functional	Intersects With	Terms of Employment	HRS-05	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	
2.1.2	N/A	+ A non-disclosure obligation is in effect. + An obligation to comply with the information security policies is in effect.	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	
2.1.2	N/A	+ A non-disclosure obligation is in effect. + An obligation to comply with the information security policies is in effect.	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	
2.1.3	N/A	+ Employees are trained and made aware.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
2.1.3	N/A	+ Employees are trained and made aware.	Functional	Subset Of	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	10	
2.1.4	N/A	+ The requirements for teleworking are determined and fulfilled. The following aspects are considered: - Secure handling of and access to information (in both electronic and paper form) while considering the protection needs and the contractual requirements applying to private (e.g. home office) and public surroundings (e.g. during travels), - Behavior in private surroundings, - Behavior in public surroundings, - Measures for protection from theft (e.g. in public surroundings), + The organization's network is accessed via a secured connection (e.g. VPN) and strong authentication.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	

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
2.1.4	N/A	+ The requirements for teleworking are determined and fulfilled. The following aspects are considered: - Secure handling of and access to information (in both electronic and paper form) while considering the protection needs and the contractual requirements applying to private (e.g. home office) and public surroundings (e.g. during travels), - Behavior in private surroundings, - Behavior in public surroundings, - Measures for protection from theft (e.g. in public surroundings), + The organization's network is accessed via a secured connection (e.g. VPN) and strong authentication.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
2.1.4	N/A	+ The requirements for teleworking are determined and fulfilled. The following aspects are considered: - Secure handling of and access to information (in both electronic and paper form) while considering the protection needs and the contractual requirements applying to private (e.g. home office) and public surroundings (e.g. during travels), - Behavior in private surroundings, - Behavior in public surroundings, - Measures for protection from theft (e.g. in public surroundings), + The organization's network is accessed via a secured connection (e.g. VPN) and strong authentication.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	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	
2.1.4	N/A	+ The requirements for teleworking are determined and fulfilled. The following aspects are considered: - Secure handling of and access to information (in both electronic and paper form) while considering the protection needs and the contractual requirements applying to private (e.g. home office) and public surroundings (e.g. during travels), - Behavior in private surroundings, - Behavior in public surroundings, - Measures for protection from theft (e.g. in public surroundings), + The organization's network is accessed via a secured connection (e.g. VPN) and strong authentication.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	
2.1.4	N/A	+ The requirements for teleworking are determined and fulfilled. The following aspects are considered: - Secure handling of and access to information (in both electronic and paper form) while considering the protection needs and the contractual requirements applying to private (e.g. home office) and public surroundings (e.g. during travels), - Behavior in private surroundings, - Behavior in public surroundings, - Measures for protection from theft (e.g. in public surroundings), + The organization's network is accessed via a secured connection (e.g. VPN) and strong authentication.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	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	
3	Physical Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.1.1	N/A	+ A security zone concept including the associated protective measures based on the requirements for the handling of information assets is in place: - Physical conditions (e.g. premises / buildings / spaces) are considered in the definition of security zones, - This also includes delivery and shipping areas. + The defined protective measures are implemented. + The code of conduct for security zones is known to all persons involved.	Functional	Equal	Zone-Based Physical Security	PES-01.2	Mechanisms exist to implement a zone-based approach to physical security.	10	
3.1.2	Superseded by 1.6.3, 5.2.8 and 5.2.9	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3.1.3	N/A	+ The requirements for the handling of supporting assets (e.g. transport, storage, repair, loss, return, disposal) are determined and fulfilled.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
3.1.3	N/A	+ The requirements for the handling of supporting assets (e.g. transport, storage, repair, loss, return, disposal) are determined and fulfilled.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
3.1.3	N/A	+ The requirements for the handling of supporting assets (e.g. transport, storage, repair, loss, return, disposal) are determined and fulfilled.	Functional	Intersects With	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that contains organizational information.	5	
3.1.3	N/A	+ The requirements for the handling of supporting assets (e.g. transport, storage, repair, loss, return, disposal) are determined and fulfilled.	Functional	Intersects With	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	5	
3.1.4	N/A	+ The requirements for mobile IT devices and mobile data storage devices are determined and fulfilled. The following aspects are considered: - Encryption, - Access protection (e.g. PIN, password), - Marking (also considering requirements for use in the presence of customers).	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
3.1.4	N/A	+ The requirements for mobile IT devices and mobile data storage devices are determined and fulfilled. The following aspects are considered: - Encryption, - Access protection (e.g. PIN, password), - Marking (also considering requirements for use in the presence of customers).	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5	
4	Identity and Access Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.1	Identity Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.1.1	N/A	+ The requirements for the handling of identification means over the entire lifecycle are determined and fulfilled. The following aspects are considered: - Creation, handover, return and destruction, - Validity periods, - Traceability, - Handling of loss.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
4.1.2	N/A	+ The procedures for user authentication have been selected based on a risk assessment. Possible attack scenarios have been considered (e.g. direct accessibility via the internet). + State of the art procedures for user authentication are applied.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
4.1.3	N/A	+ The creating, changing, and deleting of user accounts is conducted. + Unique and personalized user accounts are used. + The use of "collective accounts" is regulated (e.g. restricted to cases where traceability of actions is dispensable). + User accounts are disabled immediately after the user has resigned from or left the organization (e.g. upon termination of the employment contract). + User accounts are regularly reviewed. + The login information is provided to the user in a secure manner. + A policy for the handling of login information is defined and implemented. The following aspects are considered: - No disclosure of login information to third parties - not even to persons of authority - under observation of legal parameters - No writing down or unencrypted storing of login information - Immediate changing of login information whenever potential compromising is suspected - No use of identical login information for business and non-business purposes - Changing of temporary or initial login information following the 1st login - Requirements for the quality of authentication information (e.g. length of password, types of characters to be used). + The login information (e.g. passwords) of a personalized user account must be known to the assigned user only.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
4.1.3	N/A	+ The creating, changing, and deleting of user accounts is conducted. + Unique and personalized user accounts are used. + The use of "collective accounts" is regulated (e.g. restricted to cases where traceability of actions is dispensable). + User accounts are disabled immediately after the user has resigned from or left the organization (e.g. upon termination of the employment contract). + User accounts are regularly reviewed. + The login information is provided to the user in a secure manner. + A policy for the handling of login information is defined and implemented. The following aspects are considered: - No disclosure of login information to third parties - not even to persons of authority - under observation of legal parameters - No writing down or unencrypted storing of login information - Immediate changing of login information whenever potential compromising is suspected - No use of identical login information for business and non-business purposes - Changing of temporary or initial login information following the 1st login - Requirements for the quality of authentication information (e.g. length of password, types of characters to be used). + The login information (e.g. passwords) of a personalized user account must be known to the assigned user only.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
4.1.3	N/A	+ The creating, changing, and deleting of user accounts is conducted. + Unique and personalized user accounts are used. + The use of "collective accounts" is regulated (e.g. restricted to cases where traceability of actions is dispensable). + User accounts are disabled immediately after the user has resigned from or left the organization (e.g. upon termination of the employment contract). + User accounts are regularly reviewed. + The login information is provided to the user in a secure manner. + A policy for the handling of login information is defined and implemented. The following aspects are considered: - No disclosure of login information to third parties - not even to persons of authority - under observation of legal parameters - No writing down or unencrypted storing of login information - Immediate changing of login information whenever potential compromising is suspected - No use of identical login information for business and non-business purposes - Changing of temporary or initial login information following the 1st login - Requirements for the quality of authentication information (e.g. length of password, types of characters to be used). + The login information (e.g. passwords) of a personalized user account must be known to the assigned user only.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	
4.1.3	N/A	+ The creating, changing, and deleting of user accounts is conducted. + Unique and personalized user accounts are used. + The use of "collective accounts" is regulated (e.g. restricted to cases where traceability of actions is dispensable). + User accounts are disabled immediately after the user has resigned from or left the organization (e.g. upon termination of the employment contract). + User accounts are regularly reviewed. + The login information is provided to the user in a secure manner. + A policy for the handling of login information is defined and implemented. The following aspects are considered: - No disclosure of login information to third parties - not even to persons of authority - under observation of legal parameters - No writing down or unencrypted storing of login information - Immediate changing of login information whenever potential compromising is suspected - No use of identical login information for business and non-business purposes - Changing of temporary or initial login information following the 1st login - Requirements for the quality of authentication information (e.g. length of password, types of characters to be used). + The login information (e.g. passwords) of a personalized user account must be known to the assigned user only.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	

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
4.1.3	N/A	+ The creating, changing, and deleting of user accounts is conducted. + Unique and personalized user accounts are used. + The use of "collective accounts" is regulated (e.g. restricted to cases where traceability of actions is dispensable). + User accounts are disabled immediately after the user has resigned from or left the organization (e.g. upon termination of the employment contract). + User accounts are regularly reviewed. + The login information is provided to the user in a secure manner. + A policy for the handling of login information is defined and implemented. The following aspects are considered: - No disclosure of login information to third parties - not even to persons of authority - under observation of legal parameters - No writing down or unencrypted storing of login information - Immediate changing of login information whenever potential compromising is suspected - No use of identical login information for business and non-business purposes - Changing of temporary or initial login information following the 1st login - Requirements for the quality of authentication information (e.g. length of password, types of characters to be used). + The login information (e.g. passwords) of a personalized user account must be known to the assigned user only.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
4.2	Access Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.2.1	N/A	+ The requirements for the management of access rights (authorization) are determined and fulfilled. The following aspects are considered: - Procedure for application, verification, and approval, - Applying the minimum ("need-to-know"/"least privilege") principle. - Access rights are revoked when no longer needed + The access rights granted for normal and privileged user accounts and technical accounts are reviewed at regular intervals also within IT systems of customers.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
4.2.1	N/A	+ The requirements for the management of access rights (authorization) are determined and fulfilled. The following aspects are considered: - Procedure for application, verification, and approval, - Applying the minimum ("need-to-know"/"least privilege") principle. - Access rights are revoked when no longer needed + The access rights granted for normal and privileged user accounts and technical accounts are reviewed at regular intervals also within IT systems of customers.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	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	
4.2.1	N/A	+ The requirements for the management of access rights (authorization) are determined and fulfilled. The following aspects are considered: - Procedure for application, verification, and approval, - Applying the minimum ("need-to-know"/"least privilege") principle. - Access rights are revoked when no longer needed + The access rights granted for normal and privileged user accounts and technical accounts are reviewed at regular intervals also within IT systems of customers.	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	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.	5	
4.2.1	N/A	+ The requirements for the management of access rights (authorization) are determined and fulfilled. The following aspects are considered: - Procedure for application, verification, and approval, - Applying the minimum ("need-to-know"/"least privilege") principle. - Access rights are revoked when no longer needed + The access rights granted for normal and privileged user accounts and technical accounts are reviewed at regular intervals also within IT systems of customers.	Functional	Intersects With	Least Privilege	IAC-21	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	
4.2.1	N/A	+ The requirements for the management of access rights (authorization) are determined and fulfilled. The following aspects are considered: - Procedure for application, verification, and approval, - Applying the minimum ("need-to-know"/"least privilege") principle. - Access rights are revoked when no longer needed + The access rights granted for normal and privileged user accounts and technical accounts are reviewed at regular intervals also within IT systems of customers.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	
5	IT Security / Cyber Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1	Cryptography	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1.1	N/A	+ All cryptographic procedures used (e.g. encryption, signature, and hash algorithms, protocols) provide the security required by the respective application field according to the recognized industry standard, - to the extent legally feasible.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
5.1.2	N/A	+ The network services used to transfer information are identified and documented. + Policies and procedures in accordance with the classification requirements for the use of network services are defined and implemented. + Measures for the protection of transferred contents against unauthorized access are implemented.	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
5.1.2	N/A	+ The network services used to transfer information are identified and documented. + Policies and procedures in accordance with the classification requirements for the use of network services are defined and implemented. + Measures for the protection of transferred contents against unauthorized access are implemented.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
5.1.2	N/A	+ The network services used to transfer information are identified and documented. + Policies and procedures in accordance with the classification requirements for the use of network services are defined and implemented. + Measures for the protection of transferred contents against unauthorized access are implemented.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
5.2	Operations Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.2.1	N/A	+ Information security requirements for changes to the organization, business processes, IT systems are determined and applied.	Functional	Intersects With	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	5	
5.2.1	N/A	+ Information security requirements for changes to the organization, business processes, IT systems are determined and applied.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
5.2.2	N/A	+ The IT systems have been subjected to risk assessment in order to determine the necessity of their separation into development, testing and operational systems. + A segmentation is implemented based on the results of risk analysis.	Functional	Intersects With	Security, Compliance & Resilience Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or data protection representative in the configuration change control review process.	5	
5.2.2	N/A	+ The IT systems have been subjected to risk assessment in order to determine the necessity of their separation into development, testing and operational systems. + A segmentation is implemented based on the results of risk analysis.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
5.2.3	N/A	+ Requirements for protection against malware are determined. + Technical and organizational measures for protection against malware are defined and implemented.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
5.2.3	N/A	+ Requirements for protection against malware are determined. + Technical and organizational measures for protection against malware are defined and implemented.	Functional	Subset Of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
5.2.4	N/A	+ Information security requirements regarding the handling of event logs are determined and fulfilled. + Security-relevant requirements regarding the logging of activities of system administrators and users are determined and fulfilled. + The IT systems used are assessed regarding the necessity of logging. + When using external IT services, information on the monitoring options is obtained and considered in the assessment. + Event logs are checked regularly for rule violations and noticeable problems in compliance with the permissible legal and organizational provisions.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
5.2.4	N/A	+ Information security requirements regarding the handling of event logs are determined and fulfilled. + Security-relevant requirements regarding the logging of activities of system administrators and users are determined and fulfilled. + The IT systems used are assessed regarding the necessity of logging. + When using external IT services, information on the monitoring options is obtained and considered in the assessment. + Event logs are checked regularly for rule violations and noticeable problems in compliance with the permissible legal and organizational provisions.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
5.2.4	N/A	+ Information security requirements regarding the handling of event logs are determined and fulfilled. + Security-relevant requirements regarding the logging of activities of system administrators and users are determined and fulfilled. + The IT systems used are assessed regarding the necessity of logging. + When using external IT services, information on the monitoring options is obtained and considered in the assessment. + Event logs are checked regularly for rule violations and noticeable problems in compliance with the permissible legal and organizational provisions.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
5.2.4	N/A	+ Information security requirements regarding the handling of event logs are determined and fulfilled. + Security-relevant requirements regarding the logging of activities of system administrators and users are determined and fulfilled. + The IT systems used are assessed regarding the necessity of logging. + When using external IT services, information on the monitoring options is obtained and considered in the assessment. + Event logs are checked regularly for rule violations and noticeable problems in compliance with the permissible legal and organizational provisions.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	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	
5.2.4	N/A	+ Information security requirements regarding the handling of event logs are determined and fulfilled. + Security-relevant requirements regarding the logging of activities of system administrators and users are determined and fulfilled. + The IT systems used are assessed regarding the necessity of logging. + When using external IT services, information on the monitoring options is obtained and considered in the assessment. + Event logs are checked regularly for rule violations and noticeable problems in compliance with the permissible legal and organizational provisions.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
5.2.5	N/A	+ Information on technical vulnerabilities for the IT systems in use is gathered (e.g. information from the manufacturer, system audits, CVS database) and evaluated (e.g. Common Vulnerability Scoring System CVSS) + Potentially affected IT systems and software are identified, assessed and any vulnerabilities are addressed.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	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	
5.2.5	N/A	+ Information on technical vulnerabilities for the IT systems in use is gathered (e.g. information from the manufacturer, system audits, CVS database) and evaluated (e.g. Common Vulnerability Scoring System CVSS) + Potentially affected IT systems and software are identified, assessed and any vulnerabilities are addressed.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
5.2.5	N/A	+ Information on technical vulnerabilities for the IT systems in use is gathered (e.g. information from the manufacturer, system audits, CVS database) and evaluated (e.g. Common Vulnerability Scoring System CVSS) + Potentially affected IT systems and software are identified, assessed and any vulnerabilities are addressed.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
5.2.5	N/A	+ Information on technical vulnerabilities for the IT systems in use is gathered (e.g. information from the manufacturer, system audits, CVS database) and evaluated (e.g. Common Vulnerability Scoring System CVSS) + Potentially affected IT systems and software are identified, assessed and any vulnerabilities are addressed.	Functional	Intersects With	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
5.2.5	N/A	+ Information on technical vulnerabilities for the IT systems in use is gathered (e.g. information from the manufacturer, system audits, CVS database) and evaluated (e.g. Common Vulnerability Scoring System CVSS) + Potentially affected IT systems and software are identified, assessed and any vulnerabilities are addressed.	Functional	Intersects With	Vulnerability Exploitation Analysis	VPM-03.1	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	

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
5.2.6	N/A	+ Requirements for auditing IT systems or services are determined. + The scope of the system audit is specified in a timely manner. + System or service audits are coordinated with the operator and users of the IT systems or services. + The results of system or service audits are stored in a traceable manner and reported to the relevant management. + Measures are derived from the results.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
5.2.6	N/A	+ Requirements for auditing IT systems or services are determined. + The scope of the system audit is specified in a timely manner. + System or service audits are coordinated with the operator and users of the IT systems or services. + The results of system or service audits are stored in a traceable manner and reported to the relevant management. + Measures are derived from the results.	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
5.2.6	N/A	+ Requirements for auditing IT systems or services are determined. + The scope of the system audit is specified in a timely manner. + System or service audits are coordinated with the operator and users of the IT systems or services. + The results of system or service audits are stored in a traceable manner and reported to the relevant management. + Measures are derived from the results.	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
5.2.6	N/A	+ Requirements for auditing IT systems or services are determined. + The scope of the system audit is specified in a timely manner. + System or service audits are coordinated with the operator and users of the IT systems or services. + The results of system or service audits are stored in a traceable manner and reported to the relevant management. + Measures are derived from the results.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	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	
5.2.7	N/A	+ Requirements for the management and control of networks are determined and fulfilled. + Requirements regarding network segmentation are determined and fulfilled.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
5.2.7	N/A	+ Requirements for the management and control of networks are determined and fulfilled. + Requirements regarding network segmentation are determined and fulfilled.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
5.2.8	N/A	+ Critical IT services are identified, and business impact is considered. + Requirements and responsibilities for continuity and recovery of those IT services are known to relevant stakeholders and fulfilled.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
5.2.8	N/A	+ Critical IT services are identified, and business impact is considered. + Requirements and responsibilities for continuity and recovery of those IT services are known to relevant stakeholders and fulfilled.	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
5.2.9	N/A	+ Backup concepts exist for relevant IT systems. The following aspects are considered: - Appropriate protective measures to ensure confidentiality, integrity, and availability for data backups. + Recovery concepts exist for relevant IT services.	Functional	Subset Of	Data Backups	BCD-11	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).	10	
5.3	System acquisitions, requirement management and development	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control are:(1) Implemented correctly; and(2) Operating as intended.	5	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Authorize Technology Assets, Applications and/or Services (TAAS)	GOV-15.4	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.	5	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Assessments	IAO-02	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	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	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	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Secure Engineering Principles	SEA-01	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	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Centralized Management of Security, Compliance & Resilience Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of security, compliance and resilience controls and related processes.	5	
5.3.1	N/A	+ The information security requirements associated with the design and development of IT systems are determined and considered. + The information security requirements associated with the acquisition or extension of IT systems and IT components are determined and considered. + Information security requirements associated with changes to developed IT systems are considered. + System approval tests are carried out under consideration of the information security requirements.	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	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.	5	
5.3.2	N/A	+ Requirements regarding the information security of network services are determined and fulfilled.	Functional	Subset Of	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	10	
5.3.2	N/A	+ Requirements regarding the information security of network services are determined and fulfilled.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
5.3.2	N/A	+ Requirements regarding the information security of network services are determined and fulfilled.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required security, compliance and resilience controls for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
5.3.2	N/A	+ Requirements regarding the information security of network services are determined and fulfilled.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
5.3.3	N/A	+ A procedure for the return and secure removal of information assets from each external IT service is defined and implemented.	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
5.3.3	N/A	+ A procedure for the return and secure removal of information assets from each external IT service is defined and implemented.	Functional	Intersects With	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	5	
5.3.3	N/A	+ A procedure for the return and secure removal of information assets from each external IT service is defined and implemented.	Functional	Intersects With	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	5	

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
5.3.4	N/A	+ Effective segregation (e.g. segregation of clients) prevents access to own information by unauthorized users of other organizations.	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	5	
5.3.4	N/A	+ Effective segregation (e.g. segregation of clients) prevents access to own information by unauthorized users of other organizations.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	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	
5.3.4	N/A	+ Effective segregation (e.g. segregation of clients) prevents access to own information by unauthorized users of other organizations.	Functional	Intersects With	On-Site Client Segregation	PES-18	Mechanisms exist to ensure client-specific sensitive/regulated data is isolated from other data when client-specific sensitive/regulated data is processed or stored within multi-client workspaces.	5	
6	Supplier Relationships	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.1.1	N/A	+ Contractors and cooperation partners are subjected to a risk assessment with regard to information security. + An appropriate level of information security is ensured by contractual agreements with contractors and cooperation partners. + Where applicable, contractual agreements with clients are passed on to contractors and cooperation partners. + Compliance with contractual agreements is verified.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
6.1.1	N/A	+ Contractors and cooperation partners are subjected to a risk assessment with regard to information security. + An appropriate level of information security is ensured by contractual agreements with contractors and cooperation partners. + Where applicable, contractual agreements with clients are passed on to contractors and cooperation partners. + Compliance with contractual agreements is verified.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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).	5	
6.1.1	N/A	+ Contractors and cooperation partners are subjected to a risk assessment with regard to information security. + An appropriate level of information security is ensured by contractual agreements with contractors and cooperation partners. + Where applicable, contractual agreements with clients are passed on to contractors and cooperation partners. + Compliance with contractual agreements is verified.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
6.1.1	N/A	+ Contractors and cooperation partners are subjected to a risk assessment with regard to information security. + An appropriate level of information security is ensured by contractual agreements with contractors and cooperation partners. + Where applicable, contractual agreements with clients are passed on to contractors and cooperation partners. + Compliance with contractual agreements is verified.	Functional	Intersects With	Review of Third-Party Services	TPM-08	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	
6.1.2	N/A	+ The non-disclosure requirements are determined and fulfilled. + Requirements and procedures for applying non-disclosure agreements are known to all persons passing on information in need of protection. + Valid non-disclosure agreements are concluded prior to forwarding sensitive information. + The requirements and procedures for the use of non-disclosure agreements and the handling of information requiring protection are reviewed at regular intervals.	Functional	Equal	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	10	
7	Compliance	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.1.1	N/A	+ Legal, regulatory, and contractual provisions of relevance to information security (see examples) are determined at regular intervals. + Policies regarding compliance with the provisions are defined, implemented, and communicated to the responsible persons.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
7.1.1	N/A	+ Legal, regulatory, and contractual provisions of relevance to information security (see examples) are determined at regular intervals. + Policies regarding compliance with the provisions are defined, implemented, and communicated to the responsible persons.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
7.1.2	N/A	+ Legal and contractual information security requirements regarding the procedures and processes in the processing of personally identifiable data are determined. + Regulations regarding the compliance with legal and contractual requirements for the protection of personally identifiable data are defined and known to the entrusted persons. + Processes and procedures for the protection of personally identifiable data are considered in the information security management system.	Functional	Intersects With	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal security, compliance and resilience control system.	5	
7.1.2	N/A	+ Legal and contractual information security requirements regarding the procedures and processes in the processing of personally identifiable data are determined. + Regulations regarding the compliance with legal and contractual requirements for the protection of personally identifiable data are defined and known to the entrusted persons. + Processes and procedures for the protection of personally identifiable data are considered in the information security management system.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
7.1.2	N/A	+ Legal and contractual information security requirements regarding the procedures and processes in the processing of personally identifiable data are determined. + Regulations regarding the compliance with legal and contractual requirements for the protection of personally identifiable data are defined and known to the entrusted persons. + Processes and procedures for the protection of personally identifiable data are considered in the information security management system.	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	5	
7.1.2	N/A	+ Legal and contractual information security requirements regarding the procedures and processes in the processing of personally identifiable data are determined. + Regulations regarding the compliance with legal and contractual requirements for the protection of personally identifiable data are defined and known to the entrusted persons. + Processes and procedures for the protection of personally identifiable data are considered in the information security management system.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
8	Prototype Protection	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.1	Physical and Environmental Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.1.1	N/A	+ A security concept under consideration of the following aspects is established: - stability of outer skin, - view and sight protection, - protection against unauthorized entry and access control, - intrusion monitoring, - documented visitor management, - client segregation.	Functional	Intersects With	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	3	
8.1.1	N/A	+ A security concept under consideration of the following aspects is established: - stability of outer skin, - view and sight protection, - protection against unauthorized entry and access control, - intrusion monitoring, - documented visitor management, - client segregation.	Functional	Intersects With	Physical Security Plan (PSP)	PES-01.1	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	
8.1.2	N/A	+ Unauthorized access to properties is not possible.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
8.1.3	N/A	+ Unauthorized access to buildings/security areas is not possible.	Functional	Subset Of	Physical Access Control	PES-03	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).	10	
8.1.4	N/A	+ Unauthorized viewing of new developments needing high or very high protection is not possible.	Functional	Subset Of	Equipment Siting & Protection	PES-12	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.	10	
8.1.5	N/A	+ At least one of the following three requirements must be implemented: - mechanical locks with documented key assignment, - electronic access systems with documented authorization assignment, - personal access control including documentation.	Functional	Subset Of	Physical Security of Offices, Rooms & Facilities	PES-04	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.	10	
8.1.6	N/A	+ Intrusion monitoring of the premises to be secured is ensured: - An intrusion detection system exists which complies with DIN EN 50131 or conforms to VDS or similar and functions with alarm tracking to a certified security service or control unit (e.g., according to DIN 77200, VdS 3138), - or 24/7 guarding by a certified security service. + Alarm plans are available. + Timely alarm processing is ensured.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
8.1.6	N/A	+ Intrusion monitoring of the premises to be secured is ensured: - An intrusion detection system exists which complies with DIN EN 50131 or conforms to VDS or similar and functions with alarm tracking to a certified security service or control unit (e.g., according to DIN 77200, VdS 3138), - or 24/7 guarding by a certified security service. + Alarm plans are available. + Timely alarm processing is ensured.	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	
8.1.7	N/A	+ Registration obligation for all visitors. + Documented non-disclosure obligation prior to access. + Publication of security and visitor regulations. + Country-specific legal provisions regarding data protection are to be observed.	Functional	Equal	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	10	
8.1.8	N/A	+ Spatial separation by staff-related or technical measures is in effect according to the following aspects: - customers, and/or - projects, - where segregation is not in effect, explicit approval by the customer is required.	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	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	
8.1.8	N/A	+ Spatial separation by staff-related or technical measures is in effect according to the following aspects: - customers, and/or - projects, - where segregation is not in effect, explicit approval by the customer is required.	Functional	Intersects With	On-Site Client Segregation	PES-18	Mechanisms exist to ensure client-specific sensitive/regulated data is isolated from other data when client-specific sensitive/regulated data is processed or stored within multi-client workspaces.	5	
8.2	Organizational Requirements	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.2.1	N/A	+ A non-disclosure agreement: - between contractor and customer (company level), - with all employees and project members (personal obligation), + Country-specific legal provisions regarding data protection are to be observed.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	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).	10	
8.2.2	N/A	+ Approval by the original customer. + contractually valid non-disclosure agreement exists: - between contractor and subcontractor (company level), - with all employees and project members of the subcontractor (personal obligation). + Ensuring compliance with the security requirements of the actual customer (proof is obtained). + Proof of the subcontractor's compliance with minimum requirements for prototype protection (e.g., certificate, attestation) is provided.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	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).	10	
8.2.2	N/A	+ Approval by the original customer. + contractually valid non-disclosure agreement exists: - between contractor and subcontractor (company level), - with all employees and project members of the subcontractor (personal obligation). + Ensuring compliance with the security requirements of the actual customer (proof is obtained). + Proof of the subcontractor's compliance with minimum requirements for prototype protection (e.g., certificate, attestation) is provided.	Functional	Intersects With	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration(1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for security, compliance and resilience controls, including any flow-down requirements to subcontractors.	3	

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
8.2.2	N/A	+ Approval by the original customer. + contractually valid non-disclosure agreement exists: - between contractor and subcontractor (company level), - with all employees and project members of the subcontractor (personal obligation). + Ensuring compliance with the security requirements of the actual customer (proof is obtained). + Proof of the subcontractor's compliance with minimum requirements for prototype protection (e.g., certificate, attestation) is provided.	Functional	Intersects With	Third-Party Attestation (3PA)	TPM-05.8	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.	3	
8.2.3	N/A	+ Ensuring execution of trainings / awareness programs by the management. + Training of employees and project members when joining the project regarding the handling of prototypes. + Regular (at least annual) training of employees regarding the handling of prototypes. + Ensuring knowledge among employees and project members regarding the respective protection needs and the resulting measures within the company. + Mandatory participation of each employee and project member in the trainings and awareness measures. + The completed measures are to be documented. + The training concept for prototype protection is an integral part of the general training concept (see also control question 2.1.3 Information Security).	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
8.2.3	N/A	+ Ensuring execution of trainings / awareness programs by the management. + Training of employees and project members when joining the project regarding the handling of prototypes. + Regular (at least annual) training of employees regarding the handling of prototypes. + Ensuring knowledge among employees and project members regarding the respective protection needs and the resulting measures within the company. + Mandatory participation of each employee and project member in the trainings and awareness measures. + The completed measures are to be documented. + The training concept for prototype protection is an integral part of the general training concept (see also control question 2.1.3 Information Security).	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8	
8.2.3	N/A	+ Ensuring execution of trainings / awareness programs by the management. + Training of employees and project members when joining the project regarding the handling of prototypes. + Regular (at least annual) training of employees regarding the handling of prototypes. + Ensuring knowledge among employees and project members regarding the respective protection needs and the resulting measures within the company. + Mandatory participation of each employee and project member in the trainings and awareness measures. + The completed measures are to be documented. + The training concept for prototype protection is an integral part of the general training concept (see also control question 2.1.3 Information Security).	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-04	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	
8.2.4	N/A	+ Ensuring that the security classification and requirements in relation to the project progress are made known to each project member. + Consideration of step-by-step plans, measures for secrecy and camouflage, development policies. + The requirements are considered as a requirement regarding the information security of the project (see Controls 1.2.3 and 7.1.1 Information Security).	Functional	Intersects With	Asset Scope Classification	AST-04.1	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).	5	
8.2.4	N/A	+ Ensuring that the security classification and requirements in relation to the project progress are made known to each project member. + Consideration of step-by-step plans, measures for secrecy and camouflage, development policies. + The requirements are considered as a requirement regarding the information security of the project (see Controls 1.2.3 and 7.1.1 Information Security).	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
8.2.5	N/A	+ Responsibilities for access authorization are clearly specified and documented. + A process for new assignments, changes and revocations of access rights is in place. + Code of conduct in case of the loss/theft of access control means.	Functional	Intersects With	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
8.2.5	N/A	+ Responsibilities for access authorization are clearly specified and documented. + A process for new assignments, changes and revocations of access rights is in place. + Code of conduct in case of the loss/theft of access control means.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
8.2.5	N/A	+ Responsibilities for access authorization are clearly specified and documented. + A process for new assignments, changes and revocations of access rights is in place. + Code of conduct in case of the loss/theft of access control means.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
8.2.6	N/A	+ Approval procedures for image recording. + Specification for classification/categorization of image material. + Secure storage of image material. + Secure deletion/disposal of image material no longer required. + Secured transmission/shipping of image material to authorized recipients only.	Functional	Intersects With	Asset Scope Classification	AST-04.1	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).	5	
8.2.6	N/A	+ Approval procedures for image recording. + Specification for classification/categorization of image material. + Secure storage of image material. + Secure deletion/disposal of image material no longer required. + Secured transmission/shipping of image material to authorized recipients only.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	
8.2.6	N/A	+ Approval procedures for image recording. + Specification for classification/categorization of image material. + Secure storage of image material. + Secure deletion/disposal of image material no longer required. + Secured transmission/shipping of image material to authorized recipients only.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
8.2.6	N/A	+ Approval procedures for image recording. + Specification for classification/categorization of image material. + Secure storage of image material. + Secure deletion/disposal of image material no longer required. + Secured transmission/shipping of image material to authorized recipients only.	Functional	Intersects With	Media Storage	DCH-06	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.	5	
8.2.6	N/A	+ Approval procedures for image recording. + Specification for classification/categorization of image material. + Secure storage of image material. + Secure deletion/disposal of image material no longer required. + Secured transmission/shipping of image material to authorized recipients only.	Functional	Intersects With	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	5	
8.2.6	N/A	+ Approval procedures for image recording. + Specification for classification/categorization of image material. + Secure storage of image material. + Secure deletion/disposal of image material no longer required. + Secured transmission/shipping of image material to authorized recipients only.	Functional	Intersects With	Notice of Collection	END-13.2	Mechanisms exist to notify individuals that Personal Data (PD) is collected by sensors.	5	
8.2.7	N/A	+ Specification for carrying along (e.g., sealed/unsealed, etc.). + Specification for use (e.g., phone calls, photography, etc.).	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	
8.2.7	N/A	+ Specification for carrying along (e.g., sealed/unsealed, etc.). + Specification for use (e.g., phone calls, photography, etc.).	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
8.3	Handling of vehicles, components, and parts	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.3.1	N/A	+ A process for obtaining customer-specific requirements for the transport of vehicles, components and parts classified as requiring protection is described and implemented. + The security requirements defined by the customer are known and observed. + The logistics/transport companies explicitly approved by the customer are commissioned. + A process for reporting any security-relevant events to the customer is described and implemented.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
8.3.1	N/A	+ A process for obtaining customer-specific requirements for the transport of vehicles, components and parts classified as requiring protection is described and implemented. + The security requirements defined by the customer are known and observed. + The logistics/transport companies explicitly approved by the customer are commissioned. + A process for reporting any security-relevant events to the customer is described and implemented.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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).	5	
8.3.1	N/A	+ A process for obtaining customer-specific requirements for the transport of vehicles, components and parts classified as requiring protection is described and implemented. + The security requirements defined by the customer are known and observed. + The logistics/transport companies explicitly approved by the customer are commissioned. + A process for reporting any security-relevant events to the customer is described and implemented.	Functional	Intersects With	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5	
8.3.2	N/A	+ The customer-specific requirements for parking/storage are verifiably known and observed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.4	Requirements for trial vehicles	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.4.1	N/A	+ The requirements for using the respective camouflage are known to the project members. + Any changes to the camouflage are made upon documented agreement with the customer. + A process for the immediate reporting of any damages to the camouflage is described and implemented.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.4.2	N/A	+ A process for obtaining customer-specific requirements for the use of trial vehicles classified as requiring protection on test and trial grounds is described and implemented. + The following aspects must be known to users of test and trial grounds: - a current list of customer-approved test and trial grounds - code of conduct for ensuring undisturbed trial operation - customer-defined protective measures These are implemented.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.4.3	N/A	+ A process for obtaining customer-specific requirements for the operation of test vehicles classified as requiring protection on public roads is described and implemented. + Protective measures defined by the customer are known and observed. + The code of conduct in case of special incidents (e.g., breakdown, accident, theft...) is known and observed.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.5	Requirements for events and shootings	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.5.1	N/A	+ A process for obtaining customer-specific requirements for presentations and events involving vehicles, components or parts classified as requiring protection is described and implemented. + Established and customer-approved security concepts (organizationally, technically, staff-related). + Code of conduct in case of special incidents.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.5.2	N/A	+ A process for obtaining customer-specific requirements for film and photo shootings involving vehicles, components or parts classified as requiring protection is described and implemented. + Proof of approval for the presumably used premises. + Established and customer-approved security concepts (organizationally, technically, staff-related). + Code of conduct in case of special incidents.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control

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
9	N/A	This is intentional invisible text for technical reasons. Please do not remove this text.	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.1	Data Protection Policies	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.1.1	N/A	+ A policy is created, regularly updated, and approved by the organization's management.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
9.2	Organization of Data Protection	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.2.1	N/A	+ A data protection officer is appointed, if required by Art. 37 GDPR - Determination of whether the appointment of a data protection officer is voluntary or mandatory - otherwise determination of a data protection function or comparable + Publication of contact details (e.g. on the Internet) + Integration into the organization's structure + Exercise of the control obligations as defined in Art. 39 (1) (b) GDPR and corresponding documentation + Documentation of the data protection status and report to organization's top management + Equipped with sufficient capacities and resources - Determination of whether the data protection function is full-time or part-time - adequate professional qualification - regular professional training - access to specialist literature - support of the data protection officer by data protection coordinators in the companies organizational units, depending on the company size (e.g. marketing, sales, personnel, logistics, development, etc.)	Functional	Subset Of	Limiting Personal Data (PD) Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.	10	
9.3	Processing directory	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.3.1	N/A	+ If required by law, a register of processing activities as defined in Article 30 (1) and/or (2) GDPR (in the latter case only information relating to the order, expressly not other information/details on internal processing) exists and is up to date. - Technical and organizational measures required for processing as required by the information security questionnaire are adequatly implemented for the processing activities - There is a process description / sequence description with defined responsibilities.	Functional	Subset Of	Register As A Data Controller and/or Data Processor	PRI-15	Mechanisms exist to register as a data controller and/or data processor, including registering databases containing Personal Data (PD) with the appropriate Data Authority, when necessary.	10	
9.4	Data protection impact assessment	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.4.1	N/A	+ Processing activities that require a data protection impact assessment are known. + Data protection impact assessments are carried out. - Responsibilities/tasks and support possibilities in the context of data protection impact assessments are defined and known.	Functional	Equal	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	10	
9.5	Data transfers	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.5.1	N/A	+ Appropriate processes and workflows for the transmission of data are implemented (e.g. valid contracts within the meaning of Art. 28 GDPR, suitable transfer instruments like standard contractual clauses, transfer impact assessments, adequacy decisions) - Ensuring the consent or the right of objection of the person responsible for subcontracting	Functional	Subset Of	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	10	
9.5.2	N/A	+ Applicable contractual obligations to clients are passed on to subcontractors and cooperation partners (sub processors). + Compliance with contractual agreements is reviewed. - Contact details of the contact persons of the subcontractor are available and up to date.	Functional	Subset Of	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	10	
9.5.2	N/A	+ Applicable contractual obligations to clients are passed on to subcontractors and cooperation partners (sub processors). + Compliance with contractual agreements is reviewed. - Contact details of the contact persons of the subcontractor are available and up to date.	Functional	Intersects With	Authority To Collect, Process, Store & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the organization to collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD), either generally or in support of a specific business process.	5	
9.5.2	N/A	+ Applicable contractual obligations to clients are passed on to subcontractors and cooperation partners (sub processors). + Compliance with contractual agreements is reviewed. - Contact details of the contact persons of the subcontractor are available and up to date.	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5	
9.5.2	N/A	+ Applicable contractual obligations to clients are passed on to subcontractors and cooperation partners (sub processors). + Compliance with contractual agreements is reviewed. - Contact details of the contact persons of the subcontractor are available and up to date.	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	8	
9.5.3	N/A	+ Transfers to third countries are known and systematically recorded. - e.g. through corresponding documentation in the processing directory + Sufficient guarantees (Chapter V GDPR, consideration of decisions of the ECJ on international data transfer, Transfer Impact Assessment in case of relevance, especially in the role of data exporter) are available for data transfers. + In the case of data transfers to third countries, it is determined whether the consent of the person responsible is to be obtained for each transfer to third countries.	Functional	Subset Of	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.	10	
9.6	Handling requests and incidents	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.6.1	N/A	+ Requests from data subjects are processed in a timely manner. - Procedures are in place to assist the controller in responding to data subject requests. - Employees are trained to the effect that they must immediately contact the respective person responsible in the event of an incoming request from a data subject and coordinate the further procedure with this person.	Functional	Equal	User Feedback Management	PRI-06.4	Mechanisms exist to maintain a process to efficiently and effectively respond to requests, complaints, concerns or questions from authenticated data subjects about Personal Data (PD) the organization collects, receives, processes, stores, transmits, shares, updates and/or disposes.	10	
9.6.2	N/A	+ Data protection incidents (e.g. unauthorized access to personal data) are processed in a timely manner. + The requirements from 1.6 of the information security questionnaire also take into account data protection incidents or, alternatively, there is an emergency plan for dealing with data protection incidents. + In addition, procedures are established and documented to ensure the following aspects: - immediate notification to the respective responsible person, as far as his order is affected - Documentation of the incident handling activities - Training of employees on the defined measures/processes - Support of the respective controller in the processing of data protection incidents	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover:(1) Preparation;(2) Automated event detection or manual incident report intake;(3) Analysis;(4) Containment;(5) Eradication; and(6) Recovery.	10	
9.6.2	N/A	+ Data protection incidents (e.g. unauthorized access to personal data) are processed in a timely manner. + The requirements from 1.6 of the information security questionnaire also take into account data protection incidents or, alternatively, there is an emergency plan for dealing with data protection incidents. + In addition, procedures are established and documented to ensure the following aspects: - immediate notification to the respective responsible person, as far as his order is affected - Documentation of the incident handling activities - Training of employees on the defined measures/processes - Support of the respective controller in the processing of data protection incidents	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
9.6.2	N/A	+ Data protection incidents (e.g. unauthorized access to personal data) are processed in a timely manner. + The requirements from 1.6 of the information security questionnaire also take into account data protection incidents or, alternatively, there is an emergency plan for dealing with data protection incidents. + In addition, procedures are established and documented to ensure the following aspects: - immediate notification to the respective responsible person, as far as his order is affected - Documentation of the incident handling activities - Training of employees on the defined measures/processes - Support of the respective controller in the processing of data protection incidents	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
9.7	Human Resources	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.7.1	N/A	+ Employees whose tasks include the processing of personal data are obliged to maintain confidentiality (even beyond the duration of the employment relationship) and to comply with applicable data protection laws. - The obligation is documented	Functional	Subset Of	Terms of Employment	HRS-05	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.	10	
9.7.2	N/A	+ Employees are trained and sensitized. - Scope, frequency, and content of the training is determined according to the protection needs of the data - Employees in critical areas (e.g. IT administrators) are instructed and trained specifically for their work (e.g. specific training courses or instructions, short videos, etc.).	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
9.7.2	N/A	+ Employees are trained and sensitized. - Scope, frequency, and content of the training is determined according to the protection needs of the data - Employees in critical areas (e.g. IT administrators) are instructed and trained specifically for their work (e.g. specific training courses or instructions, short videos, etc.).	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	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	
9.8	Instructions	N/A	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.8.1	N/A	+ The instructions by the controller regarding the processing of personal data are handled. + Procedures and measures are in place to ensure that: - Received instructions are documented - Instructions can be implemented (e.g. procedures for correcting, deleting, ...) - Data is separated by client and specific order or project	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8	
9.8.1	N/A	+ The instructions by the controller regarding the processing of personal data are handled. + Procedures and measures are in place to ensure that: - Received instructions are documented - Instructions can be implemented (e.g. procedures for correcting, deleting, ...) - Data is separated by client and specific order or project	Functional	Intersects With	Secure Practices Guidelines	OPS-05	Mechanisms exist to provide guidelines and recommendations for the secure use of Technology Assets, Applications and/or Services (TAAS) to assist in the configuration, installation and use of the product and/or service.	8	