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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.1	Proportionality	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.1-1	N/A	All financial institutions should comply with the provisions set out in these guidelines in such a way that is proportionate to, and takes account of, the financial institutions' size, their internal organisation, and the nature, scope, complexity and riskiness of the services and products that the financial institutions provide or intend to provide.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	3		CPL-01
3.2	Governance and Strategy	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.2.1	Governance	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.2.1-2	N/A	The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information security risk management, and business continuity, including those for the management body and its committees.	Functional	Intersects With	Security, Compliance & Resilience Governance Policy	GOV-01	Mechanisms exist to establish a formal, documented security, compliance and resilience governance policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving	5		
3.2.1-2	N/A	The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information security risk management, and business continuity, including those for the management body and its committees.	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-02	Mechanisms exist to facilitate the design, implementation, and monitoring of security, compliance and resilience governance controls.	5		GOV-01
3.2.1-2	N/A	The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information security risk management, and business continuity, including those for the management body and its committees.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5		GOV-04
3.2.1-2	N/A	The management body should ensure that financial institutions have adequate internal governance and internal control framework in place for their ICT and security risks. The management body should set clear roles and responsibilities for ICT functions, information security risk management, and business continuity, including those for the management body and its committees.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
3.2.1-3	N/A	The management body should ensure that the quantity and skills of financial institutions' staff is adequate to support their ICT operational needs and their ICT and security risk management processes on an ongoing basis and to ensure the implementation of their ICT strategy. The management body should ensure that the allocated budget is appropriate to fulfil the above. Furthermore, financial institutions should ensure that all staff members, including key function holders, receive appropriate training on ICT and security risks, including on information security, on an annual basis, or more frequently if required (see also Section 3.4.7.)	Functional	Intersects With	Identify Critical Skills & Gaps	HRS-16	Mechanisms exist to evaluate the critical security, compliance and resilience skills needed to support the organization's mission and identify gaps that exist.	5		HRS-13
3.2.1-3	N/A	The management body should ensure that the quantity and skills of financial institutions' staff is adequate to support their ICT operational needs and their ICT and security risk management processes on an ongoing basis and to ensure the implementation of their ICT strategy. The management body should ensure that the allocated budget is appropriate to fulfil the above. Furthermore, financial institutions should ensure that all staff members, including key function holders, receive appropriate training on ICT and security risks, including on information security, on an annual basis, or more frequently if required (see also Section 3.4.7.)	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	5		PRM-03
3.2.1-3	N/A	The management body should ensure that the quantity and skills of financial institutions' staff is adequate to support their ICT operational needs and their ICT and security risk management processes on an ongoing basis and to ensure the implementation of their ICT strategy. The management body should ensure that the allocated budget is appropriate to fulfil the above. Furthermore, financial institutions should ensure that all staff members, including key function holders, receive appropriate training on ICT and security risks, including on information security, on an annual basis, or more frequently if required (see also Section 3.4.7.)	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		SAT-02
3.2.1-4	N/A	The management body has overall accountability for setting, approving and overseeing the implementation of financial institutions' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and security risks.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
3.2.1-4	N/A	The management body has overall accountability for setting, approving and overseeing the implementation of financial institutions' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and	Functional	Intersects With	Strategic Plan & Objectives	PRM-02	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5		PRM-01.1
3.2.1-4	N/A	The management body has overall accountability for setting, approving and overseeing the implementation of financial institutions' ICT strategy as part of their overall business strategy as well as for the establishment of an effective risk management framework for ICT and security risks.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	3		RSK-01
3.2.2	Strategy	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.2.2-5	The ICT strategy should be aligned with financial institutions' overall business strategy and should define:	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.2.2-5.a	N/A	How financial institutions' ICT should evolve to effectively support and participate in their business strategy, including the evolution of the organisational structure, ICT system changes and key dependencies with third parties;	Functional	Intersects With	Strategic Plan & Objectives	PRM-02	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5		PRM-01.1
3.2.2-5.a	N/A	How financial institutions' ICT should evolve to effectively support and participate in their business strategy, including the evolution of the organisational structure, ICT system changes and key dependencies with third parties;	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-04	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	3		SEA-02
3.2.2-5.b	N/A	The planned strategy and evolution of the architecture of ICT, including third-party dependencies;	Functional	Intersects With	Strategic Plan & Objectives	PRM-02	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5		PRM-01.1
3.2.2-5.b	N/A	The planned strategy and evolution of the architecture of ICT, including third-party dependencies;	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-04	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5		SEA-02
3.2.2-5.c	N/A	Clear information security objectives, focusing on ICT systems and ICT services, staff and processes	Functional	Intersects With	Control Objectives	GOV-03.3	Mechanisms exist to establish control objectives as the basis for the design, selection, implementation and management of the organization's internal security, compliance and resilience control system.	5		GOV-09
3.2.2-5.c	N/A	Clear information security objectives, focusing on ICT systems and ICT services, staff and processes	Functional	Intersects With	Strategic Plan & Objectives	PRM-02	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5		PRM-01.1

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.2.2-6	N/A	Financial institutions should establish sets of action plans that contain measures to be taken to achieve the objective of the ICT strategy. These should be communicated to all relevant staff (including contractors and third-party providers where applicable and relevant). The action plans should be periodically reviewed to ensure their relevance and appropriateness. Financial institutions should also establish processes to monitor and measure the effectiveness of the implementation of their ICT strategy.	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	3		GOV-05
3.2.2-6	N/A	Financial institutions should establish sets of action plans that contain measures to be taken to achieve the objective of the ICT strategy. These should be communicated to all relevant staff (including contractors and third-party providers where applicable and relevant). The action plans should be periodically reviewed to ensure their relevance and appropriateness. Financial institutions should also establish processes to monitor and measure the effectiveness of the implementation of their ICT strategy.	Functional	Intersects With	Strategic Plan & Objectives	PRM-02	Mechanisms exist to establish a: (1) Strategic security, compliance and resilience-specific business plan; and (2) Set of objectives to achieve that plan.	5		PRM-01.1
3.2.3	Use of Third-Party Providers	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.2.3-7	N/A	Without prejudice to Circular CSSF 22/806 on outsourcing arrangements, financial institutions should ensure the effectiveness of the risk-mitigating measures as defined by their risk management framework, including the measures set out in these guidelines, when operational functions of payment services and/or ICT services and ICT systems of any activity are outsourced, including to group entities, or when using third parties.	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
3.2.3-7	N/A	Without prejudice to Circular CSSF 22/806 on outsourcing arrangements, financial institutions should ensure the effectiveness of the risk-mitigating measures as defined by their risk management framework, including the measures set out in these guidelines, when operational functions of payment services and/or ICT services and ICT systems of any activity are outsourced, including to group entities, or when using third parties.	Functional	Intersects With	Third-Party Services	TPM-12	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-04
3.2.3-7	N/A	Without prejudice to Circular CSSF 22/806 on outsourcing arrangements, financial institutions should ensure the effectiveness of the risk-mitigating measures as defined by their risk management framework, including the measures set out in these guidelines, when operational functions of payment services and/or ICT services and ICT systems of any activity are outsourced, including to group entities, or when using third parties.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
3.2.3-8	To ensure continuity of ICT services and ICT systems, financial institutions should ensure that contracts and service level agreements (both for normal circumstances as well as in the event of service disruption - see also section 3.7.2.) with providers (outsourcing providers, group entities, or third-party providers) include the following:	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.2.3-8.a	N/A	Appropriate and proportionate information security-related objectives and measures including requirements such as minimum cybersecurity requirements; specifications of the financial institution's data life cycle; any requirements regarding data encryption, network security and security monitoring processes, and the location of data centres;	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-12.2	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5		TPM-04.4
3.2.3-8.a	N/A	Appropriate and proportionate information security-related objectives and measures including requirements such as minimum cybersecurity requirements; specifications of the financial institution's data life cycle; any requirements regarding data encryption, network security and security monitoring processes, and the location of data centres;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or	8		TPM-05
3.2.3-8.b	N/A	Operational and security incident handling procedures including escalation and reporting.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-21	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5		TPM-11
3.2.3-8.b	N/A	Operational and security incident handling procedures including escalation and reporting.	Functional	Intersects With	Security Compromise Notification Agreements	TPM-21.1	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		TPM-05.1
3.2.3-9	N/A	Financial institutions should monitor and seek assurance on the level of compliance of these providers with the security objectives, measures and performance targets of the financial institution.	Functional	Subset Of	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	10		TPM-08
3.3	ICT and Security Risk Management Framework	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.3.1	Organisation and Objectives	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.3.1-10	N/A	Financial institutions should identify and manage their ICT and security risks. The ICT function(s) in charge of ICT systems, processes and security operations should have appropriate processes and controls in place to ensure that all risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the financial institution's risk appetite and that the projects and systems they deliver and the activities they perform are in compliance with external and internal requirements.	Functional	Subset Of	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	10		RSK-01
3.3.1-10	N/A	Financial institutions should identify and manage their ICT and security risks. The ICT function(s) in charge of ICT systems, processes and security operations should have appropriate processes and controls in place to ensure that all risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the financial institution's risk appetite and that the projects and systems they deliver and the activities they perform are in compliance with external and internal requirements.	Functional	Intersects With	Risk Appetite	RSK-05.3	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	3		RSK-01.5
3.3.1-11	N/A	Financial institutions should assign the responsibility for managing and overseeing ICT and security risks to a control function. Financial institutions should ensure the independence and objectivity of this control function by appropriately segregating it from ICT operations processes. This control function should be directly accountable to the management body and responsible for monitoring and controlling adherence to the ICT and security risk management framework. It should ensure that ICT and security risks are identified, measured, assessed, managed, monitored and reported. Financial institutions should ensure that this control function is not responsible for any internal audit. The internal audit function should, following a risk-based approach, have the capacity to independently review and provide objective assurance of the compliance of all ICT and security-related activities and units of a financial institutions with the financial institution's policies and procedures and with external requirements.	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.3.1-11	N/A	Financial institutions should assign the responsibility for managing and overseeing ICT and security risks to a control function. Financial institutions should ensure the independence and objectivity of this control function by appropriately segregating it from ICT operations processes. This control function should be directly accountable to the management body and responsible for monitoring and controlling adherence to the ICT and security risk management framework. It should ensure that ICT and security risks are identified, measured, assessed, managed, monitored and reported. Financial institutions should ensure that this control function is not responsible for any internal audit. The internal audit function should, following a risk-based approach, have the capacity to independently review and provide objective assurance of the compliance of all ICT and security-related activities and units of a financial institutions with the financial institution's policies and procedures and with external requirements.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5		GOV-04
3.3.1-11	N/A	Financial institutions should assign the responsibility for managing and overseeing ICT and security risks to a control function. Financial institutions should ensure the independence and objectivity of this control function by appropriately segregating it from ICT operations processes. This control function should be directly accountable to the management body and responsible for monitoring and controlling adherence to the ICT and security risk management framework. It should ensure that ICT and security risks are identified, measured, assessed, managed, monitored and reported. Financial institutions should ensure that this control function is not responsible for any internal audit. The internal audit function should, following a risk-based approach, have the capacity to independently review and provide objective assurance of the compliance of all ICT and security-related activities and units of a financial institutions with the financial institution's policies and procedures and with external requirements.	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	3		HRS-11
3.3.1-12	N/A	Financial institutions should define and assign key roles and responsibilities, and relevant reporting lines, for the ICT and security risk management framework to be effective. This framework should be fully integrated into, and aligned with, financial institutions' overall risk management processes.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5		GOV-04
3.3.1-12	N/A	Financial institutions should define and assign key roles and responsibilities, and relevant reporting lines, for the ICT and security risk management framework to be effective. This framework should be fully integrated into, and aligned with, financial institutions' overall risk management processes.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	5		RSK-01
3.3.1-13	The ICT and security risk management framework should include processes in place to:	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.3.1-13.a	N/A	Determine the risk appetite for ICT and security risks, in accordance with the risk appetite of the financial institution;	Functional	Subset Of	Risk Appetite	RSK-05.3	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	10		RSK-01.5
3.3.1-13.b	N/A	Identify and assess the ICT and security risks to which a financial institution is exposed;	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	5		RSK-03
3.3.1-13.b	N/A	Identify and assess the ICT and security risks to which a financial institution is exposed;	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		RSK-04
3.3.1-13.c	N/A	Define mitigation measures, including controls, to mitigate ICT and security risks;	Functional	Subset Of	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	10		RSK-06
3.3.1-13.d	N/A	Monitor the effectiveness of these measures as well as the number of reported incidents, including for PSPs the incidents reported in accordance with Article 105-2 of LPS affecting the ICT-related activities, and take action to correct the measures where necessary;	Functional	Intersects With	Measures of Performance	GOV-12	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	3		GOV-05
3.3.1-13.d	N/A	Monitor the effectiveness of these measures as well as the number of reported incidents, including for PSPs the incidents reported in accordance with Article 105-2 of LPS affecting the ICT-related activities, and take action to correct the measures where necessary;	Functional	Intersects With	Risk Monitoring	RSK-22	Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and resilience controls; (2) Changes to the organization's risk profile; and (3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.	5		RSK-11
3.3.1-13.e	N/A	Report to the management body on the ICT and security risks and controls;	Functional	Subset Of	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	10		GOV-01.2
3.3.1-13.f	N/A	Identify and assess whether there are any ICT and security risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant operational or	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5		CHG-03
3.3.1-13.f	N/A	Identify and assess whether there are any ICT and security risks resulting from any major change in ICT system or ICT services, processes or procedures, and/or after any significant operational or	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-13.1	Mechanisms exist to define instances that require a risk assessment to be performed.	8		RSK-04.3
3.3.1-14	N/A	Financial institutions should ensure that the ICT and security risk management framework is documented, and continuously improved, based on "lessons learned" during its implementation and monitoring. The ICT and security risk management framework should be approved and reviewed, at least once a year, by the management body.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and	5		GOV-03
3.3.1-14	N/A	Financial institutions should ensure that the ICT and security risk management framework is documented, and continuously improved, based on "lessons learned" during its implementation and monitoring. The ICT and security risk management framework should be approved and reviewed, at least once a year, by the management body.	Functional	Intersects With	Commitment To Continual Improvements	PRM-05.1	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	5		GOV-01.3
3.3.1-14	N/A	Financial institutions should ensure that the ICT and security risk management framework is documented, and continuously improved, based on "lessons learned" during its implementation and monitoring. The ICT and security risk management framework should be approved and reviewed, at least once a year, by the management body.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	3		RSK-01
3.3.2	Identification of Functions, Processes and Assets	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.3.2-15	N/A	Financial institutions should identify, establish and maintain updated mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks.	Functional	Intersects With	Asset-Service Dependencies	AST-06	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	3		AST-01.1
3.3.2-15	N/A	Financial institutions should identify, establish and maintain updated mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks.	Functional	Intersects With	Business Process Definition	PRM-10	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5		PRM-06

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.3.2-15	N/A	Financial institutions should identify, establish and maintain updated mapping of their business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5		RSK-08
3.3.2-16	N/A	In addition, financial institutions should identify, establish and maintain updated mapping of the information assets supporting their business functions and supporting processes, such as ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes, to be able to, at least, manage the information assets that support their critical business functions and processes.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02
3.3.2-16	N/A	In addition, financial institutions should identify, establish and maintain updated mapping of the information assets supporting their business functions and supporting processes, such as ICT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes, to be able to, at least, manage the information assets that support their critical business functions and processes.	Functional	Intersects With	Asset-Service Dependencies	AST-06	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		AST-01.1
3.3.3	Classification and Risk Assessment	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.3.3-17	N/A	Financial institutions should classify the identified business functions, supporting processes and information assets referred to in paragraphs 15 and 16 in terms of criticality.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02
3.3.3-17	N/A	Financial institutions should classify the identified business functions, supporting processes and information assets referred to in paragraphs 15 and 16 in terms of criticality.	Functional	Intersects With	Risk-Based Security Categorization	RSK-07	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5		RSK-02
3.3.3-18	N/A	To define the criticality of these identified business functions, supporting processes and information assets, financial institutions should, at a minimum, consider the confidentiality, integrity and availability requirements. There should be clearly assigned accountability and responsibility for the information assets.	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment	AST-07.1	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5		AST-03
3.3.3-18	N/A	To define the criticality of these identified business functions, supporting processes and information assets, financial institutions should, at a minimum, consider the confidentiality, integrity and availability requirements. There should be clearly assigned accountability and responsibility for the information assets.	Functional	Intersects With	Data & Asset Classification	DCH-04	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5		DCH-02
3.3.3-19	N/A	Financial institutions should review the adequacy of the classification of the information assets and relevant documentation, when risk assessment is performed.	Functional	Intersects With	Data Reclassification	DCH-04.2	Mechanisms exist to reclassify data, including associated Technology Assets, Applications and/or Services (TAAS), commensurate with the security category and/or classification level of the	5		DCH-11
3.3.3-20	N/A	Financial institutions should identify the ICT and security risks that impact the identified and classified business functions, supporting processes and information assets, according to their criticality. This risk assessment should be carried out and documented annually or at shorter intervals if required. Such risk assessments should also be performed on any major changes in infrastructure, processes or procedures affecting the business functions, supporting processes or information assets, and consequently the current risk assessment of financial institutions should be updated.	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8		RSK-04
3.3.3-20	N/A	Financial institutions should identify the ICT and security risks that impact the identified and classified business functions, supporting processes and information assets, according to their criticality. This risk assessment should be carried out and documented annually or at shorter intervals if required. Such risk assessments should also be performed on any major changes in infrastructure, processes or procedures affecting the business functions, supporting processes or information assets, and consequently the current risk assessment of financial institutions should be updated.	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-13.1	Mechanisms exist to define instances that require a risk assessment to be performed.	5		RSK-04.3
3.3.3-20	N/A	Financial institutions should identify the ICT and security risks that impact the identified and classified business functions, supporting processes and information assets, according to their criticality. This risk assessment should be carried out and documented annually or at shorter intervals if required. Such risk assessments should also be performed on any major changes in infrastructure, processes or procedures affecting the business functions, supporting processes or information assets, and consequently the current risk assessment of financial institutions should be updated.	Functional	Intersects With	Risk Assessment Update	RSK-13.2	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	5		RSK-07
3.3.3-21	N/A	Financial institutions should ensure that they continuously monitor threats and vulnerabilities relevant to their business processes, supporting functions and information assets and should regularly review the risk scenarios impacting them.	Functional	Intersects With	Risk Monitoring	RSK-22	Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and resilience controls; (2) Changes to the organization's risk profile; and (3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.	3		RSK-11
3.3.3-21	N/A	Financial institutions should ensure that they continuously monitor threats and vulnerabilities relevant to their business processes, supporting functions and information assets and should regularly review the risk scenarios impacting them.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5		THR-01
3.3.3-21	N/A	Financial institutions should ensure that they continuously monitor threats and vulnerabilities relevant to their business processes, supporting functions and information assets and should regularly review the risk scenarios impacting them.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	5		VPM-01
3.3.4	Risk Mitigation	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.3.4-22	N/A	Based on the risk assessments, financial institutions should determine which measures are required to mitigate identified ICT and security risks to acceptable levels and whether changes are necessary to the existing business processes, control measures, ICT systems and ICT services. A financial institution should consider the time required to implement these changes and the time to take appropriate interim mitigating measures to minimise ICT and security risks to stay within the financial institution's ICT and security risk appetite.	Functional	Intersects With	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	8		RSK-06
3.3.4-22	N/A	Based on the risk assessments, financial institutions should determine which measures are required to mitigate identified ICT and security risks to acceptable levels and whether changes are necessary to the existing business processes, control measures, ICT systems and ICT services. A financial institution should consider the time required to implement these changes and the time to take appropriate interim mitigating measures to minimise ICT and security risks to stay within the financial institution's ICT and security risk appetite.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-17.1	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5		RSK-06.4
3.3.4-23	N/A	Financial institutions should define and implement measures to mitigate identified ICT and security risks and to protect information assets in accordance with their classification.	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	5		DCH-01

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.3.4-23	N/A	Financial institutions should define and implement measures to mitigate identified ICT and security risks and to protect information assets in accordance with their classification.	Functional	Intersects With	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	5		RSK-06
3.3.5	Reporting	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.3.5-24	N/A	Financial institutions should report risk assessment results to the management body in a clear and timely manner. Such reporting is without prejudice to the obligation of PSPs to provide competent authorities with an updated and comprehensive risk assessment, as laid down in Article 105-1(2) of LPS.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	8		GOV-01.2
3.3.6	Audit	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.3.6-25	N/A	A financial institution's governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks and in payments (for PSPs) to provide independent assurance of their effectiveness to the management body. The auditors should be independent within or from the financial institution. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.	Functional	Intersects With	Internal Audit Function	CPL-07.1	Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities.	5		CPL-02.1
3.3.6-25	N/A	A financial institution's governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks and in payments (for PSPs) to provide independent assurance of their effectiveness to the management body. The auditors should be independent within or from the financial institution. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5		CPL-02.2
3.3.6-25	N/A	A financial institution's governance, systems and processes for its ICT and security risks should be audited on a periodic basis by auditors with sufficient knowledge, skills and expertise in ICT and security risks and in payments (for PSPs) to provide independent assurance of their effectiveness to the management body. The auditors should be independent within or from the financial institution. The frequency and focus of such audits should be commensurate with the relevant ICT and security risks.	Functional	Intersects With	Assessment Team Subject Matter Expertise	CPL-09	Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable: (1) Professional qualifications to perform the audit and/or assessment; and (2) Subject matter expertise to perform review, interview and test activities for in-scope People, Processes, Technologies, Data and/or Facilities (PPTDF).	5		CPL-01.6
3.3.6-26	N/A	A financial institution's management body should approve the audit plan, including any ICT audits and any material modifications thereto. The audit plan and its execution, including the audit frequency, should reflect and be proportionate to the inherent ICT and security risks in the financial institution and should be updated regularly.	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	3		CPL-02.2
3.3.6-26	N/A	A financial institution's management body should approve the audit plan, including any ICT audits and any material modifications thereto. The audit plan and its execution, including the audit frequency, should reflect and be proportionate to the inherent ICT and security risks in the financial institution and should be updated regularly.	Functional	Intersects With	Audit Planning Activities	CPL-07.3	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	5		CPL-04
3.3.6-27	N/A	A formal follow-up process including provisions for the timely verification and remediation of critical ICT audit findings should be established.	Functional	Intersects With	Non-Conformity Corrective Action	CPL-06.1	Mechanisms exist to implement corrective action to remediate instances of non-conformity with applicable statutory, regulatory, and/or contractual compliance obligations.	8		CPL-02.3
3.3.6-27	N/A	A formal follow-up process including provisions for the timely verification and remediation of critical ICT audit findings should be established.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
3.4	Information Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.1	Information Security Policy	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.1-28	N/A	Financial institutions should develop and document an information security policy that should define the high-level principles and rules to protect the confidentiality, integrity and availability of financial institutions' and their customers' data and information. The information security policy should be in line with the financial institution's information security objectives and based on the relevant results of the risk assessment process. The policy should be approved by the management body.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8		GOV-02
3.4.1-29	N/A	The policy should include a description of the main roles and responsibilities of information security management, and it should set out the requirements for staff and contractors, processes and technology in relation to information security, recognising that staff and contractors at all levels have responsibilities in ensuring financial institutions' information security. The policy should ensure the confidentiality, integrity and availability of a financial institution's critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy should be communicated to all staff and contractors of the financial	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
3.4.1-29	N/A	The policy should include a description of the main roles and responsibilities of information security management, and it should set out the requirements for staff and contractors, processes and technology in relation to information security, recognising that staff and contractors at all levels have responsibilities in ensuring financial institutions' information security. The policy should ensure the confidentiality, integrity and availability of a financial institution's critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy should be communicated to all staff and contractors of the financial	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	3		GOV-04
3.4.1-29	N/A	The policy should include a description of the main roles and responsibilities of information security management, and it should set out the requirements for staff and contractors, processes and technology in relation to information security, recognising that staff and contractors at all levels have responsibilities in ensuring financial institutions' information security. The policy should ensure the confidentiality, integrity and availability of a financial institution's critical logical and physical assets, resources and sensitive data whether at rest, in transit or in use. The information security policy should be communicated to all staff and contractors of the financial	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-08.2	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	3		HRS-05.7
3.4.1-30	Based on the information security policy, financial institutions should establish and implement security measures to mitigate the ICT and security risks that they are exposed to. These measures should include:	N/A	Functional	No Relationship	N/A	N/A	N/A	0		

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.4.1-30.a	N/A	organisation and governance in accordance with paragraphs 10 and 11;	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
3.4.1-30.a	N/A	organisation and governance in accordance with paragraphs 10 and 11;	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5		GOV-04
3.4.1-30.b	N/A	logical security (Section 3.4.2);	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
3.4.1-30.c	N/A	physical security (Section 3.4.3);	Functional	Intersects With	Physical & Environmental Protections	PES-02	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5		PES-01
3.4.1-30.d	N/A	ICT operations security (Section 3.4.4);	Functional	Subset Of	Security Operations Policy	OPS-01	Mechanisms exist to establish a formal, documented security operations policy that:	10		
3.4.1-30.d	N/A	ICT operations security (Section 3.4.4);	Functional	Intersects With	Operations Security	OPS-02	Mechanisms exist to facilitate the implementation of operational security controls.	5		OPS-01
3.4.1-30.e	N/A	security monitoring (Section 3.4.5);	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
3.4.1-30.f	N/A	information security reviews, assessment and testing (Section 3.4.6);	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5		IAO-02
3.4.1-30.g	N/A	information security training and awareness (Section 3.4.7).	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-02	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	3		SAT-01
3.4.1-30.g	N/A	information security training and awareness (Section 3.4.7).	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		SAT-02
3.4.2	Logical Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.2-31	Financial institutions should define, document and implement procedures for logical access control (identity and access management). These procedures should be implemented, enforced, monitored and periodically reviewed. The procedures should also include controls for monitoring anomalies. These procedures should, at a minimum, implement the following elements, where the term 'user' also includes	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.2-31.a	N/A	Need to know, least privilege and segregation of duties: financial institutions should manage access rights to information assets and their supporting systems on a 'need-to-know' basis, including for remote access. Users should be granted minimum access rights that are strictly required to execute their duties (principle of 'least privilege'), i.e. to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5		HRS-11
3.4.2-31.a	N/A	Need to know, least privilege and segregation of duties: financial institutions should manage access rights to information assets and their supporting systems on a 'need-to-know' basis, including for remote access. Users should be granted minimum access rights that are strictly required to execute their duties (principle of 'least privilege'), i.e. to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		IAC-20
3.4.2-31.a	N/A	Need to know, least privilege and segregation of duties: financial institutions should manage access rights to information assets and their supporting systems on a 'need-to-know' basis, including for remote access. Users should be granted minimum access rights that are strictly required to execute their duties (principle of 'least privilege'), i.e. to prevent unjustified access to a large set of data or to prevent the allocation of combinations of access rights that may be used to circumvent controls (principle of 'segregation of duties').	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8		IAC-21
3.4.2-31.b	N/A	User accountability: financial institutions should limit, as much as possible, the use of generic and shared user accounts and ensure that users can be identified for the actions performed in the ICT systems.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-21	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	8		IAC-15.5
3.4.2-31.b	N/A	User accountability: financial institutions should limit, as much as possible, the use of generic and shared user accounts and ensure that users can be identified for the actions performed in the ICT systems.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-32	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5		IAC-02
3.4.2-31.c	N/A	Privileged access rights: financial institutions should implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access entitlements (e.g. administrator accounts). In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	8		IAC-16
3.4.2-31.c	N/A	Privileged access rights: financial institutions should implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access entitlements (e.g. administrator accounts). In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used.	Functional	Intersects With	Multi-Factor Authentication (MFA) For Network Access to Privileged Accounts	IAC-37.5	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5		IAC-06.1
3.4.2-31.c	N/A	Privileged access rights: financial institutions should implement strong controls over privileged system access by strictly limiting and closely supervising accounts with elevated system access entitlements (e.g. administrator accounts). In order to ensure secure communication and reduce risk, remote administrative access to critical ICT systems should be granted only on a need-to-know basis and when strong authentication solutions are used.	Functional	Intersects With	Remote Access Privileged Commands & Sensitive Data Access	NET-26.6	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	5		NET-14.4

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

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

Focal Document: **Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)**
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.4.2-31.d	N/A	Logging of user activities: at a minimum, all activities by privileged users should be logged and monitored. Access logs should be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with Section 3.3.3, without prejudice to the retention requirements set out in EU and national law. A financial institution should use this information to facilitate the identification and investigation of anomalous activities that have been detected in the provision of	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	5		MON-08
3.4.2-31.d	N/A	Logging of user activities: at a minimum, all activities by privileged users should be logged and monitored. Access logs should be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with Section 3.3.3, without prejudice to the retention requirements set out in EU and national law. A financial institution should use this information to facilitate the identification and investigation of anomalous activities that have been detected in the provision of	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5		MON-10
3.4.2-31.d	N/A	Logging of user activities: at a minimum, all activities by privileged users should be logged and monitored. Access logs should be secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, supporting processes and information assets, in accordance with Section 3.3.3, without prejudice to the retention requirements set out in EU and national law. A financial institution should use this information to facilitate the identification and investigation of anomalous activities that have been detected in the provision of	Functional	Intersects With	Privileged Functions Logging	MON-14	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5		MON-03.3
3.4.2-31.e	N/A	Access management: access rights should be granted, withdrawn or modified in a timely manner, according to predefined approval workflows that involve the business owner of the information being accessed (information asset owner). In the case of termination of employment, access rights should be promptly withdrawn.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-04	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	8		IAC-07
3.4.2-31.e	N/A	Access management: access rights should be granted, withdrawn or modified in a timely manner, according to predefined approval workflows that involve the business owner of the information being accessed (information asset owner). In the case of termination of employment, access rights should be promptly withdrawn.	Functional	Intersects With	Termination of Employment	IAC-04.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5		IAC-07.2
3.4.2-31.e	N/A	Access management: access rights should be granted, withdrawn or modified in a timely manner, according to predefined approval workflows that involve the business owner of the information being accessed (information asset owner). In the case of termination of employment, access rights should be promptly withdrawn.	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-09	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5		IAC-28.1
3.4.2-31.f	N/A	Access recertification: access rights should be periodically reviewed to ensure that users do not possess excessive privileges and that access rights are withdrawn when no longer required.	Functional	Subset Of	Periodic Review of Individual & Service Account Privileges	IAC-12	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as	10		IAC-17
3.4.2-31.g	N/A	Authentication methods: financial institutions should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, information or the process being accessed. This should, at a minimum, include complex passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5		IAC-10.1
3.4.2-31.g	N/A	Authentication methods: financial institutions should enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with. Authentication methods should be commensurate with the criticality of ICT systems, information or the process being accessed. This should, at a minimum, include complex passwords or stronger authentication methods (such as two-factor authentication), based on relevant risk.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	5		IAC-06
3.4.2-32	N/A	Electronic access by applications to data and ICT systems should be limited to a minimum required to provide the relevant service.	Functional	Intersects With	Least Privilege	IAC-30	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business	5		IAC-21
3.4.3	Physical Security	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.3-33	N/A	Financial institutions' physical security measures should be defined, documented and implemented to protect their premises, data centres and sensitive areas from unauthorised access and from environmental hazards.	Functional	Subset Of	Physical & Environmental Security Policy	PES-01	Mechanisms exist to establish a formal, documented physical and environmental security policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected	10		
3.4.3-33	N/A	Financial institutions' physical security measures should be defined, documented and implemented to protect their premises, data centres and sensitive areas from unauthorised access and from environmental hazards.	Functional	Subset Of	Physical & Environmental Protections	PES-02	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10		PES-01
3.4.3-34	N/A	Physical access to ICT systems should be permitted to only authorised individuals. Authorisation should be assigned in accordance with the individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access rights are promptly revoked when not required.	Functional	Intersects With	Physical Access Authorizations	PES-06	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	8		PES-02
3.4.3-34	N/A	Physical access to ICT systems should be permitted to only authorised individuals. Authorisation should be assigned in accordance with the individual's tasks and responsibilities and limited to individuals who are appropriately trained and monitored. Physical access should be regularly reviewed to ensure that unnecessary access rights are promptly revoked when not required.	Functional	Intersects With	Physical Access Control	PES-08	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5		PES-03
3.4.3-35	N/A	Adequate measures to protect from environmental hazards should be commensurate with the importance of the buildings and the criticality of the operations or ICT systems located in these buildings.	Functional	Intersects With	Physical & Environmental Protections	PES-02	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5		PES-01
3.4.4	ICT Operations	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.4-36	Financial institutions should implement procedures to prevent the occurrence of security issues in ICT systems and ICT services and should minimise their impact on ICT service delivery. These procedures should include the following measures:	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.4-36.a	N/A	identification of potential vulnerabilities, which should be evaluated and remediated by ensuring that software and firmware are up to date, including the software provided by financial institutions to their internal and external users, by deploying critical security patches or by implementing compensating controls;	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8		VPM-02
3.4.4-36.a	N/A	identification of potential vulnerabilities, which should be evaluated and remediated by ensuring that software and firmware are up to date, including the software provided by financial institutions to their internal and external users, by deploying critical security patches or by implementing compensating controls;	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.4.4-36.a	N/A	identification of potential vulnerabilities, which should be evaluated and remediated by ensuring that software and firmware are up to date, including the software provided by financial institutions to their internal and external users, by deploying critical security patches or by implementing compensating controls;	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
3.4.4-36.b	N/A	implementation of secure configuration baselines of all network components;	Functional	Subset Of	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	10		CFG-02
3.4.4-36.c	N/A	implementation of network segmentation, data loss prevention systems and the encryption of network traffic (in accordance with the data classification);	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
3.4.4-36.c	N/A	implementation of network segmentation, data loss prevention systems and the encryption of network traffic (in accordance with the data classification);	Functional	Intersects With	Data Loss Prevention (DLP)	DCH-40	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and	5		NET-17
3.4.4-36.c	N/A	implementation of network segmentation, data loss prevention systems and the encryption of network traffic (in accordance with the data classification);	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06
3.4.4-36.d	N/A	implementation of protection of endpoints including servers, workstations and mobile devices; financial institutions should evaluate whether endpoints meet the security standards defined by them before they are granted access to the corporate network;	Functional	Intersects With	Endpoint Protection Mechanisms	END-03	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5		END-02
3.4.4-36.d	N/A	implementation of protection of endpoints including servers, workstations and mobile devices; financial institutions should evaluate whether endpoints meet the security standards defined by them before they are granted access to the corporate network;	Functional	Intersects With	Remote Access Endpoint Security Validation	NET-26.3	Automated mechanisms exist to validate the security posture of the endpoint devices (e.g., software versions and patch levels) prior to allowing devices to connect to organizational Technology Assets, Applications and/or Services (TAAS).	5		NET-14.7
3.4.4-36.e	N/A	ensuring that mechanisms are in place to verify the integrity of software, firmware and data;	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-11	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5		END-06
3.4.4-36.e	N/A	ensuring that mechanisms are in place to verify the integrity of software, firmware and data;	Functional	Intersects With	Software / Firmware Integrity Verification	TDA-20.3	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	3		TDA-14.1
3.4.4-36.f	N/A	encryption of data at rest and in transit (in accordance with the data classification).	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
3.4.4-36.f	N/A	encryption of data at rest and in transit (in accordance with the data classification).	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	5		CRY-05
3.4.4-37	N/A	Furthermore, on an ongoing basis, financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks appropriately. These changes should be part of the financial institutions' formal change management process, which should ensure that changes are properly planned, tested, documented, authorised and deployed.	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	8		CHG-01
3.4.4-37	N/A	Furthermore, on an ongoing basis, financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks appropriately. These changes should be part of the financial institutions' formal change management process, which should ensure that changes are properly planned, tested, documented, authorised and deployed.	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	5		CHG-02
3.4.4-37	N/A	Furthermore, on an ongoing basis, financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require adoption of additional measures to mitigate related risks appropriately. These changes should be part of the financial institutions' formal change management process, which should ensure that changes are properly planned, tested, documented, authorised and deployed.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5		CHG-03
3.4.5	Security Monitoring	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.5-38	Financial institutions should establish and implement policies and procedures to detect anomalous activities that may impact financial institutions' information security and to respond to these events appropriately. As part of this continuous monitoring, financial institutions should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets. The continuous	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.5-38.a	N/A	relevant internal and external factors, including business and ICT administrative functions;	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
3.4.5-38.a	N/A	relevant internal and external factors, including business and ICT administrative functions;	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		MON-16
3.4.5-38.b	N/A	transactions to detect misuse of access by third parties or other entities and internal misuse of access;	Functional	Intersects With	Insider Threats	MON-17.3	Mechanisms exist to monitor internal personnel activity for potential security incidents.	5		MON-16.1
3.4.5-38.b	N/A	transactions to detect misuse of access by third parties or other entities and internal misuse of access;	Functional	Intersects With	Third-Party Threats	MON-17.4	Mechanisms exist to monitor third-party personnel activity for potential security incidents.	5		MON-16.2
3.4.5-38.c	N/A	potential internal and external threats.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		MON-16
3.4.5-38.c	N/A	potential internal and external threats.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	3		THR-01

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.4.5-39	N/A	Financial institutions should establish and implement processes and organisation structures to identify and constantly monitor security threats that could materially affect their abilities to provide services. Financial institutions should actively monitor technological developments to ensure that they are aware of security risks. Financial institutions should implement detective measures, for instance to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and should check for corresponding new security updates.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	3		END-04
3.4.5-39	N/A	Financial institutions should establish and implement processes and organisation structures to identify and constantly monitor security threats that could materially affect their abilities to provide services. Financial institutions should actively monitor technological developments to ensure that they are aware of security risks. Financial institutions should implement detective measures, for instance to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and should check for corresponding new security updates.	Functional	Intersects With	Monitoring For Information Disclosure	MON-19	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	5		MON-11
3.4.5-39	N/A	Financial institutions should establish and implement processes and organisation structures to identify and constantly monitor security threats that could materially affect their abilities to provide services. Financial institutions should actively monitor technological developments to ensure that they are aware of security risks. Financial institutions should implement detective measures, for instance to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and should check for corresponding new security updates.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5		THR-01
3.4.5-40	N/A	The security monitoring process should also help a financial institution to understand the nature of operational or security incidents, to identify trends and to support the organisation's investigations.	Functional	Intersects With	Incident Pattern Analysis	IRO-17.1	Mechanisms exist to analyze historical incidents in aggregate to identify: (1) Patterns; (2) Trends; and (3) Other common root causes in order to address the vulnerability and risk.	5		IRO-09.4
3.4.5-40	N/A	The security monitoring process should also help a financial institution to understand the nature of operational or security incidents, to identify trends and to support the organisation's investigations.	Functional	Intersects With	Trend Analysis Reporting	MON-06.1	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.	5		MON-06.2
3.4.6	Information Security Reviews, Assessment and Testing	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.6-41	N/A	Financial institutions should perform a variety of information security reviews, assessments and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, financial institutions may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the institution should consider good practices such as source code reviews, vulnerability assessments, penetration tests and red team	Functional	Intersects With	Periodic Audits	CPL-07.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5		CPL-02.2
3.4.6-41	N/A	Financial institutions should perform a variety of information security reviews, assessments and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, financial institutions may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the institution should consider good practices such as source code reviews, vulnerability assessments, penetration tests and red team	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5		IAO-02
3.4.6-41	N/A	Financial institutions should perform a variety of information security reviews, assessments and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, financial institutions may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the institution should consider good practices such as source code reviews, vulnerability assessments, penetration tests and red team	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
3.4.6-41	N/A	Financial institutions should perform a variety of information security reviews, assessments and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, financial institutions may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the institution should consider good practices such as source code reviews, vulnerability assessments, penetration tests and red team	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
3.4.6-41	N/A	Financial institutions should perform a variety of information security reviews, assessments and testing to ensure the effective identification of vulnerabilities in their ICT systems and ICT services. For instance, financial institutions may perform gap analysis against information security standards, compliance reviews, internal and external audits of the information systems, or physical security reviews. Furthermore, the institution should consider good practices such as source code reviews, vulnerability assessments, penetration tests and red team	Functional	Intersects With	Red Team Exercises	VPM-21	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	3		VPM-10
3.4.6-42	N/A	Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and ICT and security risk assessment process.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-02	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10		IAO-01
3.4.6-42	N/A	Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and ICT and security risk assessment process.	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5		IAO-02
3.4.6-42	N/A	Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and ICT and security risk assessment process.	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	3		THR-10
3.4.6-42	N/A	Financial institutions should establish and implement an information security testing framework that validates the robustness and effectiveness of their information security measures and ensure that this framework considers threats and vulnerabilities, identified through threat monitoring and ICT and security risk assessment process.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	5		VPM-01
3.4.6-43	The information security testing framework should ensure that tests:	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.4.6-43.a	N/A	are carried out by independent testers with sufficient knowledge, skills and expertise in testing information security measures and who are not involved in the development of the information security measures;	Functional	Intersects With	Assessment Team Subject Matter Expertise	CPL-09	Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable: (1) Professional qualifications to perform the audit and/or assessment; and (2) Subject matter expertise to perform review, interview and test activities for in-scope People, Processes, Technologies, Data and/or Facilities (PPTDF).	5		CPL-01.6

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.4.6-43.a	N/A	are carried out by independent testers with sufficient knowledge, skills and expertise in testing information security measures and who are not involved in the development of the information security measures;	Functional	Intersects With	Assessor Independence	IAO-06	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct security, compliance and/or resilience control assessments.	5		IAO-02.1
3.4.6-43.a	N/A	are carried out by independent testers with sufficient knowledge, skills and expertise in testing information security measures and who are not involved in the development of the information security measures;	Functional	Intersects With	Independent Penetration Agent or Team	VPM-19	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5		VPM-07.1
3.4.6-43.b	N/A	include vulnerability scans and penetration tests (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
3.4.6-43.b	N/A	include vulnerability scans and penetration tests (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
3.4.6-43.b	N/A	include vulnerability scans and penetration tests (including threat-led penetration testing where necessary and appropriate) commensurate to the level of risk identified with the business processes and systems.	Functional	Intersects With	Red Team Exercises	VPM-21	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	3		VPM-10
3.4.6-44	N/A	Financial institutions should perform ongoing and repeated tests of the security measures. For all critical ICT systems (paragraph 17), these tests should be performed at least on an annual basis and, for PSPs, they will be part of the comprehensive assessment of the security risks related to the payment services they provide, in accordance with Article 105-1(2) of LPS. Non-critical systems should be tested regularly using a risk-based approach, but at least every 3 years.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-05.1	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5		CPL-03.2
3.4.6-44	N/A	Financial institutions should perform ongoing and repeated tests of the security measures. For all critical ICT systems (paragraph 17), these tests should be performed at least on an annual basis and, for PSPs, they will be part of the comprehensive assessment of the security risks related to the payment services they provide, in accordance with Article 105-1(2) of LPS. Non-critical systems should be tested regularly using a risk-based approach, but at least every 3 years.	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5		IAO-02
3.4.6-44	N/A	Financial institutions should perform ongoing and repeated tests of the security measures. For all critical ICT systems (paragraph 17), these tests should be performed at least on an annual basis and, for PSPs, they will be part of the comprehensive assessment of the security risks related to the payment services they provide, in accordance with Article 105-1(2) of LPS. Non-critical systems should be tested regularly using a risk-based approach, but at least every 3 years.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	3		VPM-06
3.4.6-45	N/A	Financial institutions should ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed internet-facing critical applications.	Functional	Intersects With	Control Functionality Verification	CHG-09	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	5		CHG-06
3.4.6-45	N/A	Financial institutions should ensure that tests of security measures are conducted in the event of changes to infrastructure, processes or procedures and if changes are made because of major operational or security incidents or due to the release of new or significantly changed internet-facing critical applications.	Functional	Intersects With	Control Validation Testing (CVT)	IAO-04	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	3		IAO-02
3.4.6-46	N/A	Financial institutions should monitor and evaluate the results of the security tests and update their security measures accordingly without undue delays in the case of critical ICT systems.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	5		IAO-05
3.4.6-46	N/A	Financial institutions should monitor and evaluate the results of the security tests and update their security measures accordingly without undue delays in the case of critical ICT systems.	Functional	Intersects With	Risk Response	RSK-16	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.	5		RSK-06.1
3.4.6-47	N/A	For PSPs, the testing framework should also encompass the security measures relevant to (1) payment terminals and devices used for the provision of payment services, (2) payment terminals and devices used for authenticating the payment service users (PSU), and (3) devices and software provided by the PSP to the PSU to generate/receive an authentication code.	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-21	Mechanisms exist to appropriately protect devices that capture sensitive and/or regulated data from tampering and substitution via direct physical interaction.	3		AST-07
3.4.6-47	N/A	For PSPs, the testing framework should also encompass the security measures relevant to (1) payment terminals and devices used for the provision of payment services, (2) payment terminals and devices used for authenticating the payment service users (PSU), and (3) devices and software provided by the PSP to the PSU to generate/receive an authentication code.	Functional	Intersects With	Embedded Technology Reviews	EMB-13	Mechanisms exist to perform evaluations of deployed embedded technologies as needed, or at least on an annual basis, to ensure that necessary updates to mitigate the risks associated with legacy embedded technologies are identified and implemented.	3		EMB-10
3.4.6-47	N/A	For PSPs, the testing framework should also encompass the security measures relevant to (1) payment terminals and devices used for the provision of payment services, (2) payment terminals and devices used for authenticating the payment service users (PSU), and (3) devices and software provided by the PSP to the PSU to generate/receive an authentication code.	Functional	Intersects With	Specialized Assessments	IAO-05	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT and OT); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or (12) Other Technology Assets, Applications and/or Services (TAAS) that require specialized expertise to determine conformity with security, compliance and/or resilience requirements.	5		IAO-02.2
3.4.6-48	N/A	Based on the security threats observed and the changes made, testing should be performed to incorporate scenarios of relevant and known potential attacks.	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	8		THR-10
3.4.6-48	N/A	Based on the security threats observed and the changes made, testing should be performed to incorporate scenarios of relevant and known potential attacks.	Functional	Intersects With	Red Team Exercises	VPM-21	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	3		VPM-10
3.4.7	Information Security Training and	N/A	Functional	No Relationship	N/A	N/A	N/A	0		

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.4.7-49	N/A	Financial institutions should establish a training programme, including periodic security awareness programmes, for all staff and contractors to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and how to address information security-related risks. Financial institutions should ensure that the training programme provides training for all staff members and contractors at least annually.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-02	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5		SAT-01
3.4.7-49	N/A	Financial institutions should establish a training programme, including periodic security awareness programmes, for all staff and contractors to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and how to address information security-related risks. Financial institutions should ensure that the training programme provides training for all staff members and contractors at least annually.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8		SAT-02
3.4.7-49	N/A	Financial institutions should establish a training programme, including periodic security awareness programmes, for all staff and contractors to ensure that they are trained to perform their duties and responsibilities consistent with the relevant security policies and procedures to reduce human error, theft, fraud, misuse or loss and how to address information security-related risks. Financial institutions should ensure that the training programme provides training for all staff members and contractors at least annually.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03
3.5	ICT Operations Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.5-50	N/A	Financial institutions should manage their ICT operations based on documented and implemented processes and procedures that are approved by the management body. This set of documents should define how financial institutions operate, monitor and control their ICT systems and services, including the documenting of critical ICT operations and should enable financial institutions to maintain up-to-date ICT asset inventory.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	3		AST-02
3.5-50	N/A	Financial institutions should manage their ICT operations based on documented and implemented processes and procedures that are approved by the management body. This set of documents should define how financial institutions operate, monitor and control their ICT systems and services, including the documenting of critical ICT operations and should enable financial institutions to maintain up-to-date ICT asset inventory.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
3.5-50	N/A	Financial institutions should manage their ICT operations based on documented and implemented processes and procedures that are approved by the management body. This set of documents should define how financial institutions operate, monitor and control their ICT systems and services, including the documenting of critical ICT operations and should enable financial institutions to maintain up-to-date ICT asset inventory.	Functional	Intersects With	Operations Security	OPS-02	Mechanisms exist to facilitate the implementation of operational security controls.	5		OPS-01
3.5-50	N/A	Financial institutions should manage their ICT operations based on documented and implemented processes and procedures that are approved by the management body. This set of documents should define how financial institutions operate, monitor and control their ICT systems and services, including the documenting of critical ICT operations and should enable financial institutions to maintain up-to-date ICT asset inventory.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-04	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5		OPS-01.1
3.5-51	N/A	Financial institutions should ensure that performance of their ICT operations is aligned to their business requirements. Financial institutions should maintain and improve, when possible, efficiency of their ICT operations, including but not limited to the need to consider how to minimise potential errors arising from the execution of manual tasks.	Functional	Intersects With	Capacity & Performance Management	CAP-02	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	3		CAP-01
3.5-51	N/A	Financial institutions should ensure that performance of their ICT operations is aligned to their business requirements. Financial institutions should maintain and improve, when possible, efficiency of their ICT operations, including but not limited to the need to consider how to minimise potential errors arising from the execution of manual tasks.	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-05	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5		OPS-03
3.5-52	N/A	Financial institutions should implement logging and monitoring procedures for critical ICT operations to allow the detection, analysis and correction of errors.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
3.5-52	N/A	Financial institutions should implement logging and monitoring procedures for critical ICT operations to allow the detection, analysis and correction of errors.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	3		MON-01.8
3.5-53	N/A	Financial institutions should maintain an up-to-date inventory of their ICT assets (including ICT systems, network devices, databases, etc.). The ICT asset inventory should store the configuration of the ICT assets and the links and interdependencies between the different ICT assets, to enable a proper configuration and change management process.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02
3.5-53	N/A	Financial institutions should maintain an up-to-date inventory of their ICT assets (including ICT systems, network devices, databases, etc.). The ICT asset inventory should store the configuration of the ICT assets and the links and interdependencies between the different ICT assets, to enable a proper configuration and change management process.	Functional	Intersects With	Asset-Service Dependencies	AST-06	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	3		AST-01.1
3.5-53	N/A	Financial institutions should maintain an up-to-date inventory of their ICT assets (including ICT systems, network devices, databases, etc.). The ICT asset inventory should store the configuration of the ICT assets and the links and interdependencies between the different ICT assets, to enable a proper configuration and change management process.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-08.1	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8		AST-02.9
3.5-54	N/A	The ICT asset inventory should be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification and ownership. Interdependencies between assets should be documented to help in the response to security and operational incidents, including cyber-attacks.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5		AST-02

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

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

Focal Document: **Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)**
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.5-54	N/A	The ICT asset inventory should be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification and ownership. Interdependencies between assets should be documented to help in the response to security and operational incidents, including cyber-attacks.	Functional	Intersects With	Asset-Service Dependencies	AST-06	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	3		AST-01.1
3.5-54	N/A	The ICT asset inventory should be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification and ownership. Interdependencies between assets should be documented to help in the response to security and operational incidents, including cyber-attacks.	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment	AST-07.1	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	3		AST-03
3.5-54	N/A	The ICT asset inventory should be sufficiently detailed to enable the prompt identification of an ICT asset, its location, security classification and ownership. Interdependencies between assets should be documented to help in the response to security and operational incidents, including cyber-attacks.	Functional	Intersects With	Comprehensive Asset Inventory Management	AST-08	Mechanisms exist to maintain a dynamically updated inventory of Technology Assets, Applications, Services and/or Data (TAASD) that provides a highly contextualized understanding of every asset that is capable of providing operational visibility required to: (1) Detect anomalies; (2) Manage complex vulnerabilities;	8		
3.5-55	N/A	Financial institutions should monitor and manage the life cycles of ICT assets, to ensure that they continue to meet and support business and risk management requirements. Financial institutions should monitor whether their ICT assets are supported by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated.	Functional	Intersects With	Technology Lifecycle Management	AST-37	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5		SEA-07.1
3.5-55	N/A	Financial institutions should monitor and manage the life cycles of ICT assets, to ensure that they continue to meet and support business and risk management requirements. Financial institutions should monitor whether their ICT assets are supported by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated.	Functional	Intersects With	Technical Debt Reviews	AST-38	Mechanisms exist to conduct ongoing "technical debt" reviews of hardware and software technologies to remediate outdated and/or unsupported technologies.	3		SEA-02.3
3.5-55	N/A	Financial institutions should monitor and manage the life cycles of ICT assets, to ensure that they continue to meet and support business and risk management requirements. Financial institutions should monitor whether their ICT assets are supported by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required	5		TDA-17
3.5-55	N/A	Financial institutions should monitor and manage the life cycles of ICT assets, to ensure that they continue to meet and support business and risk management requirements. Financial institutions should monitor whether their ICT assets are supported by their external or internal vendors and developers and whether all relevant patches and upgrades are applied based on documented processes. The risks stemming from outdated or unsupported ICT assets should be assessed and mitigated.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
3.5-56	N/A	Financial institutions should implement performance and capacity planning and monitoring processes to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner.	Functional	Intersects With	Capacity & Performance Management	CAP-02	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	8		CAP-01
3.5-56	N/A	Financial institutions should implement performance and capacity planning and monitoring processes to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner.	Functional	Intersects With	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5		CAP-03
3.5-56	N/A	Financial institutions should implement performance and capacity planning and monitoring processes to prevent, detect and respond to important performance issues of ICT systems and ICT capacity shortages in a timely manner.	Functional	Intersects With	Performance Monitoring	CAP-05	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical Technology Assets, Applications and/or Services (TAAS).	5		CAP-04
3.5-57	N/A	Financial institutions should define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups should be set out in line with business recovery requirements and the criticality of the data and the ICT systems and evaluated according to the performed risk assessment. Testing of the backup and restoration procedures should be undertaken on a periodic basis.	Functional	Intersects With	Data Backups	BCD-24	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8		BCD-11
3.5-57	N/A	Financial institutions should define and implement data and ICT systems backup and restoration procedures to ensure that they can be recovered as required. The scope and frequency of backups should be set out in line with business recovery requirements and the criticality of the data and the ICT systems and evaluated according to the performed risk assessment. Testing of the backup and restoration procedures should be undertaken on a periodic basis.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	5		BCD-11.1
3.5-58	N/A	Financial institutions should ensure that data and ICT system backups are stored securely and are sufficiently remote from the primary site so they are not exposed to the same risks.	Functional	Intersects With	Separation from Primary Storage Site	BCD-12.1	Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats.	8		BCD-08.1
3.5-58	N/A	Financial institutions should ensure that data and ICT system backups are stored securely and are sufficiently remote from the primary site so they are not exposed to the same risks.	Functional	Intersects With	Alternate Storage Site	BCD-12	Mechanisms exist to establish an alternate storage site that stores both the assets and necessary agreements needed for the recovery of Technology Assets, Applications, Services and/or Data (TAASD).	5		BCD-08
3.5-58	N/A	Financial institutions should ensure that data and ICT system backups are stored securely and are sufficiently remote from the primary site so they are not exposed to the same risks.	Functional	Intersects With	Separate Storage for Critical Information	BCD-24.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5		BCD-11.2
3.5.1	ICT Incident and Problem Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.5.1-59	N/A	Financial institutions should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and to enable financial institutions to continue or resume, in a timely manner, critical business functions and processes when disruptions occur. Financial institutions should determine appropriate criteria and thresholds for classifying events as operational or security incidents, as set out in the 'Definitions' section of this circular, as well as early warning indicators that should serve as alerts to enable early detection of these incidents.	Functional	Intersects With	Incident Response Operations	IRO-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5		IRO-01
3.5.1-59	N/A	Financial institutions should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and to enable financial institutions to continue or resume, in a timely manner, critical business functions and processes when disruptions occur. Financial institutions should determine appropriate criteria and thresholds for classifying events as operational or security incidents, as set out in the 'Definitions' section of this circular, as well as early warning indicators that should serve as alerts to enable early detection of these incidents.	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5		IRO-02.4
3.5.1-59	N/A	Financial institutions should establish and implement an incident and problem management process to monitor and log operational and security ICT incidents and to enable financial institutions to continue or resume, in a timely manner, critical business functions and processes when disruptions occur. Financial institutions should determine appropriate criteria and thresholds for classifying events as operational or security incidents, as set out in the 'Definitions' section of this circular, as well as early warning indicators that should serve as alerts to enable early detection of these incidents.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-05	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	3		IRO-03

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.5.1-60	To minimise the impact of adverse events and enable timely recovery, financial institutions should establish appropriate processes and organisational structures to ensure a consistent and integrated monitoring, handling and follow-up of operational and security incidents and to make sure that the root causes are identified and eliminated to prevent the occurrence of repeated incidents. The incident and problem management	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.5.1-60.a	N/A	the procedures to identify, track, log, categorise and classify incidents according to a priority, based on business criticality;	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	8		IRO-02.4
3.5.1-60.a	N/A	the procedures to identify, track, log, categorise and classify incidents according to a priority, based on business criticality;	Functional	Intersects With	Incident Tracking Repository	IRO-17	Mechanisms exist to maintain a repository of cybersecurity events and incidents that documents: (1) Details of the incident (e.g., category, severity and affected parties); (2) Remediation actions taken through incident closure; and (3) A summary from the Root Cause Analysis (RCA), if applicable.	3		IRO-09.3
3.5.1-60.b	N/A	the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	3		IRO-04
3.5.1-60.b	N/A	the roles and responsibilities for different incident scenarios (e.g. errors, malfunctioning, cyber-attacks);	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5		IRO-07
3.5.1-60.c	N/A	problem management procedures to identify, analyse and solve the root cause behind one or more incidents - a financial institution should analyse operational or security incidents likely to affect the financial institution that have been identified or have occurred within and/or outside the organisation and should consider key lessons learned from these analyses and update the security measures accordingly;	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	8		IRO-13
3.5.1-60.c	N/A	problem management procedures to identify, analyse and solve the root cause behind one or more incidents - a financial institution should analyse operational or security incidents likely to affect the financial institution that have been identified or have occurred within and/or outside the organisation and should consider key lessons learned from these analyses and update the security measures accordingly;	Functional	Intersects With	Incident Pattern Analysis	IRO-17.1	Mechanisms exist to analyze historical incidents in aggregate to identify: (1) Patterns; (2) Trends; and (3) Other common root causes in order to address the vulnerability and risk.	5		IRO-09.4
3.5.1-60.d	N/A	effective internal communication plans, including incident notification and escalation procedures - also covering security-related customer complaints - to ensure that: (i) incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant senior management and ICT senior management; (ii) the management body is informed on an ad hoc basis in the event of significant incidents and, at least, informed of the impact, the response and the additional controls to be defined as a result of the incidents.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
3.5.1-60.d	N/A	effective internal communication plans, including incident notification and escalation procedures - also covering security-related customer complaints - to ensure that: (i) incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant senior management and ICT senior management; (ii) the management body is informed on an ad hoc basis in the event of significant incidents and, at least, informed of the impact, the response and the additional controls to be defined as a result of the incidents.	Functional	Intersects With	Situational Awareness For Incidents	IRO-16.1	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5		IRO-09
3.5.1-60.d	N/A	effective internal communication plans, including incident notification and escalation procedures - also covering security-related customer complaints - to ensure that: (i) incidents with a potentially high adverse impact on critical ICT systems and ICT services are reported to the relevant senior management and ICT senior management; (ii) the management body is informed on an ad hoc basis in the event of significant incidents and, at least, informed of the impact, the response and the additional controls to be defined as a result of the incidents.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Review Escalation Matrix	MON-05.3	Mechanisms exist to make event log and security-relevant telemetry review processes more efficient and effective by developing and maintaining an incident response escalation matrix.	3		MON-17.1
3.5.1-60.e	N/A	incident response procedures to mitigate the impacts related to the incidents and to ensure that the service becomes operational and secure in a timely manner;	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8		IRO-02
3.5.1-60.e	N/A	incident response procedures to mitigate the impacts related to the incidents and to ensure that the service becomes operational and secure in a timely manner;	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	3		IRO-04
3.5.1-60.f	N/A	specific external communication plans for critical business functions and processes in order to: (i) collaborate with relevant stakeholders to effectively respond to and recover from the incident; (ii) provide timely information to external parties (e.g. customers, other market participants, the supervisory authority) as appropriate and in line with an applicable regulation.	Functional	Intersects With	Correlation with External Organizations	IRO-06.1	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	3		IRO-02.5
3.5.1-60.f	N/A	specific external communication plans for critical business functions and processes in order to: (i) collaborate with relevant stakeholders to effectively respond to and recover from the incident; (ii) provide timely information to external parties (e.g. customers, other market participants, the supervisory authority) as appropriate and in line with an applicable regulation.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8		IRO-10
3.6	ICT Project and Change Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.6.1	ICT Project Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.6.1-61	N/A	A financial institution should implement a programme and/or a project governance process that defines roles, responsibilities and accountabilities to effectively support the implementation of the ICT strategy.	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-04	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	5		PRM-01
3.6.1-61	N/A	A financial institution should implement a programme and/or a project governance process that defines roles, responsibilities and accountabilities to effectively support the implementation of the ICT strategy.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	3		PRM-04

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.6.1-62	N/A	A financial institution should appropriately monitor and mitigate risks deriving from their portfolio of ICT projects (programme management), considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.	Functional	Intersects With	Security, Compliance & Resilience Protection Portfolio Management	PRM-04	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	5		PRM-01
3.6.1-62	N/A	A financial institution should appropriately monitor and mitigate risks deriving from their portfolio of ICT projects (programme management), considering also risks that may result from interdependencies between different projects and from dependencies of multiple projects on the same resources and/or expertise.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	5		PRM-04
3.6.1-63	A financial institution should establish and implement an ICT project management policy that includes as a minimum:	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.6.1-63.a	N/A	project objectives;	Functional	Subset Of	Project & Resource Management Policy	PRM-01	Mechanisms exist to establish a formal, documented project and resource management policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected behaviors; (3) Is reviewed at least annually; and (4) Is updated, as necessary, to adapt to evolving	10		
3.6.1-63.a	N/A	project objectives;	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	3		PRM-04
3.6.1-63.b	N/A	roles and responsibilities;	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	3		HRS-03
3.6.1-63.b	N/A	roles and responsibilities;	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	3		PRM-04
3.6.1-63.c	N/A	a project risk assessment;	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	5		PRM-04
3.6.1-63.c	N/A	a project risk assessment;	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	3		RSK-04
3.6.1-63.d	N/A	a project plan, timeframe and steps;	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	3		PRM-04
3.6.1-63.e	N/A	key milestones;	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	3		PRM-04
3.6.1-63.f	N/A	change management requirements.	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	5		CHG-01
3.6.1-63.f	N/A	change management requirements.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	3		PRM-04
3.6.1-64	N/A	The ICT project management policy should ensure that information security requirements are analysed and approved by a function that is independent from the development function.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-09	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	5		PRM-05
3.6.1-64	N/A	The ICT project management policy should ensure that information security requirements are analysed and approved by a function that is independent from the development function.	Functional	Intersects With	Software Design Review	TDA-05.4	Mechanisms exist to have an independent review of the software design to validate: (1) Applicable security, compliance and resilience requirements are met; and (2) Identified risks are remediated.	5		TDA-06.5
3.6.1-65	N/A	A financial institution should ensure that all areas impacted by an ICT project are represented in the project team and that the project team has the knowledge required to ensure secure and successful project implementation.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	3		HRS-03.2
3.6.1-65	N/A	A financial institution should ensure that all areas impacted by an ICT project are represented in the project team and that the project team has the knowledge required to ensure secure and successful project implementation.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	3		PRM-04
3.6.1-66	N/A	The establishment and progress of ICT projects and their associated risks should be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, regularly and on an ad hoc basis as appropriate. Financial institutions should include project risk in their risk management framework.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2
3.6.1-66	N/A	The establishment and progress of ICT projects and their associated risks should be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, regularly and on an ad hoc basis as appropriate. Financial institutions should include project risk in their risk management framework.	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-08	Mechanisms exist to assess security, compliance and resilience controls as part of Technology Assets, Applications and/or Services (TAAS) project development to determine whether controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting requirements.	3		PRM-04

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.6.1-66	N/A	The establishment and progress of ICT projects and their associated risks should be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, regularly and on an ad hoc basis as appropriate. Financial institutions should include project risk in their risk management framework.	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	3		RSK-01
3.6.2	ICT Systems Acquisition and Development	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.6.2-67	N/A	Financial institutions should develop and implement a process governing the acquisition, development and maintenance of ICT systems. This process should be designed using a risk-based approach.	Functional	Intersects With	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5		PRM-07
3.6.2-67	N/A	Financial institutions should develop and implement a process governing the acquisition, development and maintenance of ICT systems. This process should be designed using a risk-based approach.	Functional	Intersects With	Technology Development & Acquisition Policy	TDA-01	Mechanisms exist to establish a formal, documented technology development and acquisition policy that: (1) Conveys executive management's intent; (2) Provides organizational direction and expected	8		PRM-07
3.6.2-67	N/A	Financial institutions should develop and implement a process governing the acquisition, development and maintenance of ICT systems. This process should be designed using a risk-based approach.	Functional	Intersects With	Technology Development & Acquisition	TDA-02	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	8		TDA-01
3.6.2-68	N/A	A financial institution should ensure that, before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined and approved by the relevant business management.	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-09	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	8		PRM-05
3.6.2-68	N/A	A financial institution should ensure that, before any acquisition or development of ICT systems takes place, the functional and non-functional requirements (including information security requirements) are clearly defined and approved by the relevant business management.	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-11.1	Mechanisms exist to design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	5		TDA-02
3.6.2-69	N/A	A financial institution should ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.	Functional	Intersects With	Access Restriction For Change	CHG-04.1	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5		CHG-04
3.6.2-69	N/A	A financial institution should ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-05	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	3		TDA-06
3.6.2-69	N/A	A financial institution should ensure that measures are in place to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development and implementation in the production environment.	Functional	Intersects With	Secure Development Environments	TDA-15	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5		TDA-07
3.6.2-70	N/A	Financial institutions should have a methodology in place for testing and approval of ICT systems prior to their first use. This methodology should consider the criticality of business processes and assets. The testing should ensure that new ICT systems perform as intended. They should also use test environments that adequately reflect the production environment.	Functional	Intersects With	Test, Validate & Document Changes	CHG-07	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented into production.	3		CHG-02.2
3.6.2-70	N/A	Financial institutions should have a methodology in place for testing and approval of ICT systems prior to their first use. This methodology should consider the criticality of business processes and assets. The testing should ensure that new ICT systems perform as intended. They should also use test environments that adequately reflect the production environment.	Functional	Intersects With	Security Authorization	IAO-14	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5		IAO-07
3.6.2-70	N/A	Financial institutions should have a methodology in place for testing and approval of ICT systems prior to their first use. This methodology should consider the criticality of business processes and assets. The testing should ensure that new ICT systems perform as intended. They should also use test environments that adequately reflect the production environment.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	5		TDA-09
3.6.2-71	N/A	Financial institutions should test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-17	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and	5		TDA-09
3.6.2-71	N/A	Financial institutions should test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
3.6.2-71	N/A	Financial institutions should test ICT systems, ICT services and information security measures to identify potential security weaknesses, violations and incidents.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07
3.6.2-72	N/A	A financial institution should implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, a financial institution should ensure the segregation of production environments from development, testing and other non-production environments. A financial institution should ensure the integrity and confidentiality of production data in non-production environments. Access to production data is restricted to authorised users.	Functional	Intersects With	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-28	Mechanisms exist to minimize the use of sensitive and/or regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	3		DCH-18.2
3.6.2-72	N/A	A financial institution should implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, a financial institution should ensure the segregation of production environments from development, testing and other non-production environments. A financial institution should ensure the integrity and confidentiality of production data in non-production environments. Access to production data is restricted to authorised users.	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-15.1	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS).	8		TDA-08
3.6.2-72	N/A	A financial institution should implement separate ICT environments to ensure adequate segregation of duties and to mitigate the impact of unverified changes to production systems. Specifically, a financial institution should ensure the segregation of production environments from development, testing and other non-production environments. A financial institution should ensure the integrity and confidentiality of production data in non-production environments. Access to production data is restricted to authorised users.	Functional	Intersects With	Use of Live Data	TDA-18	Mechanisms exist to approve, document and control the use of live data in development and test environments.	5		TDA-10

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.6.2-73	N/A	Financial institutions should implement measures to protect the integrity of the source codes of ICT systems that are developed in-house. They should also document the development, implementation, operation and/or configuration of the ICT systems comprehensively to reduce any unnecessary dependency on subject matter experts. The documentation of the ICT system should contain, where applicable, at least user documentation, technical system documentation and operating procedures.	Functional	Intersects With	Administrator Documentation	TDA-08.3	Mechanisms exist to obtain, protect and distribute administrator documentation for Technology Assets, Applications and/or Services (TAAS) that describe: (1) Secure configuration, installation and operation of the TAAS; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5		TDA-04
3.6.2-73	N/A	Financial institutions should implement measures to protect the integrity of the source codes of ICT systems that are developed in-house. They should also document the development, implementation, operation and/or configuration of the ICT systems comprehensively to reduce any unnecessary dependency on subject matter experts. The documentation of the ICT system should contain, where applicable, at least user documentation, technical system documentation and operating procedures.	Functional	Intersects With	Access to Program Source Code	TDA-16.1	Mechanisms exist to limit privileges to change software resident within software libraries.	5		TDA-20
3.6.2-74	N/A	A financial institution's processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside the ICT organisation (e.g. end user computing applications) using a risk-based approach. The financial institution should maintain a register of these applications that support critical business functions or processes.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	3		AST-02
3.6.2-74	N/A	A financial institution's processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside the ICT organisation (e.g. end user computing applications) using a risk-based approach. The financial institution should maintain a register of these applications that support critical business functions or processes.	Functional	Intersects With	Shadow Information Technology Detection	OPS-09	Mechanisms exist to detect the presence of unauthorized Technology Assets, Applications and/or Services (TAAS) in use.	3		OPS-07
3.6.2-74	N/A	A financial institution's processes for acquisition and development of ICT systems should also apply to ICT systems developed or managed by the business function's end users outside the ICT organisation (e.g. end user computing applications) using a risk-based approach. The financial institution should maintain a register of these applications that support critical business functions or processes.	Functional	Intersects With	Technology Development & Acquisition	TDA-02	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	3		TDA-01
3.6.3	ICT Change Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.6.3-75	N/A	Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner. Financial institutions should handle the changes during emergencies (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards.	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	8		CHG-01
3.6.3-75	N/A	Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner. Financial institutions should handle the changes during emergencies (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards.	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	5		CHG-02
3.6.3-75	N/A	Financial institutions should establish and implement an ICT change management process to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner. Financial institutions should handle the changes during emergencies (i.e. changes that must be introduced as soon as possible) following procedures that provide adequate safeguards.	Functional	Intersects With	Emergency Changes	CHG-10	Mechanisms exist to govern change management procedures for "emergency" changes.	5		CHG-07
3.6.3-76	N/A	Financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require the adoption of additional measures to mitigate the risks involved. These changes should be in accordance with the financial institutions' formal change management process.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-06	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	8		CHG-03
3.6.3-76	N/A	Financial institutions should determine whether changes in the existing operational environment influence the existing security measures or require the adoption of additional measures to mitigate the risks involved. These changes should be in accordance with the financial institutions' formal change management process.	Functional	Intersects With	Control Functionality Verification	CHG-09	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	3		CHG-06
3.7	Business Continuity Management	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.7-77	N/A	Financial institutions should establish a sound business continuity management (BCM) process to maximise their abilities to provide services on an ongoing basis and to limit losses in the event of severe business disruption.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	10		BCD-01
3.7.1	Business Impact Analysis	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.7.1-78	N/A	As part of sound business continuity management, financial institutions should conduct business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (e.g. third-party provider data relevant to a business process or publicly available data that may be relevant to the BIA) and scenario analysis. The BIA should also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies, in accordance with Section 3.3.3.	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5		BCD-02
3.7.1-78	N/A	As part of sound business continuity management, financial institutions should conduct business impact analysis (BIA) by analysing their exposure to severe business disruptions and assessing their potential impacts (including on confidentiality, integrity and availability), quantitatively and qualitatively, using internal and/or external data (e.g. third-party provider data relevant to a business process or publicly available data that may be relevant to the BIA) and scenario analysis. The BIA should also consider the criticality of the identified and classified business functions, supporting processes, third parties and information assets, and their interdependencies, in accordance with Section 3.3.3.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	8		RSK-08
3.7.1-79	N/A	Financial institutions should ensure that their ICT systems and ICT services are designed and aligned with their BIA, for example with redundancy of certain critical components to prevent disruptions caused by events impacting those components.	Functional	Intersects With	Operational Resilience Capabilities	BCD-03	Mechanisms exist to ensure capabilities are implemented to provide operational resilience to: (1) Unintentional errors; and (2) Intentional attack or circumvention.	3		SEA-01.3
3.7.1-79	N/A	Financial institutions should ensure that their ICT systems and ICT services are designed and aligned with their BIA, for example with redundancy of certain critical components to prevent disruptions caused by events impacting those components.	Functional	Intersects With	Redundant Secondary System	BCD-21	Mechanisms exist to maintain a failover capability, which is not collocated with the primary Technology Asset, Application and/or Service (TAAS), which can be activated with little-to-no loss of information or disruption to operations.	3		BCD-11.7
3.7.1-79	N/A	Financial institutions should ensure that their ICT systems and ICT services are designed and aligned with their BIA, for example with redundancy of certain critical components to prevent disruptions caused by events impacting those components.	Functional	Intersects With	Achieving Security, Compliance & Resilience Requirements	SEA-02.1	Mechanisms exist to design Technology Assets, Applications and/or Services (TAAS) so that required capabilities continue to operate in a controlled and acceptable manner, when conditions are both routine and degraded.	5		SEA-01.2

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

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

Focal Document: **Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)**
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.7.2	Business Continuity Planning	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.7.2-80	N/A	Based on their BIAs, financial institutions should establish plans to ensure business continuity (business continuity plans, BCPs), which should be documented and approved by their management bodies. The plans should specifically consider risks that could adversely impact ICT systems and ICT services. The plans should support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets. Financial institutions should coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and (2) Adverse conditions.	5		BCD-01
3.7.2-80	N/A	Based on their BIAs, financial institutions should establish plans to ensure business continuity (business continuity plans, BCPs), which should be documented and approved by their management bodies. The plans should specifically consider risks that could adversely impact ICT systems and ICT services. The plans should support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets. Financial institutions should coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	8		BCD-01.7
3.7.2-80	N/A	Based on their BIAs, financial institutions should establish plans to ensure business continuity (business continuity plans, BCPs), which should be documented and approved by their management bodies. The plans should specifically consider risks that could adversely impact ICT systems and ICT services. The plans should support objectives to protect and, if necessary, re-establish the confidentiality, integrity and availability of their business functions, supporting processes and information assets. Financial institutions should coordinate with relevant internal and external stakeholders, as appropriate, during the establishment of these plans.	Functional	Intersects With	Coordinate with Related Plans	BCD-07.3	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	3		BCD-01.1
3.7.2-81	N/A	Financial institutions should put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident). In cases of severe business disruption that trigger specific business continuity plans, financial institutions should prioritise business continuity actions using risk-based approach, which can be based on the risk assessments carried out under Section 3.3.3. For PSPs this may include, for example, facilitating the further processing of critical transactions while remediation efforts continue.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5		BCD-01.7
3.7.2-81	N/A	Financial institutions should put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident). In cases of severe business disruption that trigger specific business continuity plans, financial institutions should prioritise business continuity actions using risk-based approach, which can be based on the risk assessments carried out under Section 3.3.3. For PSPs this may include, for example, facilitating the further processing of critical transactions while remediation efforts continue.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8		BCD-01.4
3.7.2-81	N/A	Financial institutions should put BCPs in place to ensure that they can react appropriately to potential failure scenarios and that they are able to recover the operations of their critical business activities after disruptions within a recovery time objective (RTO, the maximum time within which a system or process must be restored after an incident) and a recovery point objective (RPO, the maximum time period during which it is acceptable for data to be lost in the event of an incident). In cases of severe business disruption that trigger specific business continuity plans, financial institutions should prioritise business continuity actions using risk-based approach, which can be based on the risk assessments carried out under Section 3.3.3. For PSPs this may include, for example, facilitating the further processing of critical transactions while remediation efforts continue.	Functional	Intersects With	Transaction Recovery	BCD-26	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based Technology Assets, Applications and/or Services (TAAS) in accordance with Recovery Point Objectives (RPOs).	3		BCD-12.1
3.7.2-82	N/A	A financial institution should consider a range of different scenarios in its BCP, including extreme but plausible ones to which it might be exposed, including a cyber-attack scenario, and it should assess the potential impact that such scenarios might have. Based on these scenarios, a financial institution should describe how the continuity of ICT systems and services, as well as the financial institution's information security, are ensured.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5		BCD-01.7
3.7.2-82	N/A	A financial institution should consider a range of different scenarios in its BCP, including extreme but plausible ones to which it might be exposed, including a cyber-attack scenario, and it should assess the potential impact that such scenarios might have. Based on these scenarios, a financial institution should describe how the continuity of ICT systems and services, as well as the financial institution's information security, are ensured.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	3		RSK-08
3.7.3	Response and Recovery Plans	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.7.3-83	N/A	Based on the BIAs (paragraph 78) and plausible scenarios (paragraph 82), financial institutions should develop response and recovery plans. These plans should specify what conditions may prompt activation of the plans and what actions should be taken to ensure the availability, continuity and recovery of, at least, financial institutions' critical ICT systems and ICT services. The response and recovery plans should aim to meet the recovery objectives of financial institutions' operations.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5		BCD-01.7
3.7.3-83	N/A	Based on the BIAs (paragraph 78) and plausible scenarios (paragraph 82), financial institutions should develop response and recovery plans. These plans should specify what conditions may prompt activation of the plans and what actions should be taken to ensure the availability, continuity and recovery of, at least, financial institutions' critical ICT systems and ICT services. The response and recovery plans should aim to meet the recovery objectives of financial institutions' operations.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	3		BCD-01.4
3.7.3-83	N/A	Based on the BIAs (paragraph 78) and plausible scenarios (paragraph 82), financial institutions should develop response and recovery plans. These plans should specify what conditions may prompt activation of the plans and what actions should be taken to ensure the availability, continuity and recovery of, at least, financial institutions' critical ICT systems and ICT services. The response and recovery plans should aim to meet the recovery objectives of financial institutions' operations.	Functional	Intersects With	Recovery Operations Criteria	BCD-05	Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recovery (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-01.5
3.7.3-84	The response and recovery plans should consider both short-term and long-term recovery options. The plans should:	N/A	Functional	No Relationship	N/A	N/A	N/A	0		

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

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

Focal Document: Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.7.3-84.a	N/A	focus on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of financial institutions and on the financial system, including on payment systems and on payment service users, and to ensure execution of pending payment transactions;	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-08.1	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration of primary processing and/or storage sites is performed.	5		BCD-02.2
3.7.3-84.a	N/A	focus on the recovery of the operations of critical business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of financial institutions and on the financial system, including on payment systems and on payment service users, and to ensure execution of pending payment transactions;	Functional	Intersects With	Transaction Recovery	BCD-26	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based Technology Assets, Applications and/or Services (TAAS) in accordance with Recovery Point Objectives (RPOs).	3		BCD-12.1
3.7.3-84.b	N/A	be documented and made available to the business and support units and readily accessible in the event of an emergency;	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse conditions.	5		BCD-01.7
3.7.3-84.c	N/A	be updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities.	Functional	Intersects With	Ongoing Contingency Planning	BCD-07	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services); (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing	8		BCD-06
3.7.3-84.c	N/A	be updated in line with lessons learned from incidents, tests, new risks identified and threats, and changed recovery objectives and priorities.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-11	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5		BCD-05
3.7.3-85	N/A	The plans should also consider alternative options where recovery may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances.	Functional	Intersects With	Inability to Return to Primary Site	BCD-16	Mechanisms exist to plan and prepare for both natural and manmade circumstances that would prevent return to the primary site.	3		BCD-09.5
3.7.3-85	N/A	The plans should also consider alternative options where recovery may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	3		BCD-07
3.7.3-86	N/A	Furthermore, as part of the response and recovery plans, a financial institution should consider and implement continuity measures to mitigate failures of third-party providers, which are of key importance for a financial institution's ICT service continuity (in line with the provisions of the Circular CSSF 22/806 on outsourcing arrangements regarding business continuity plans).	Functional	Intersects With	Coordinate With External Service Providers	BCD-07.4	Mechanisms exist to coordinate internal contingency plans with those of external service providers to ensure that organizational resiliency requirements can be satisfied.	5		BCD-01.2
3.7.3-86	N/A	Furthermore, as part of the response and recovery plans, a financial institution should consider and implement continuity measures to mitigate failures of third-party providers, which are of key importance for a financial institution's ICT service continuity (in line with the provisions of the Circular CSSF 22/806 on outsourcing arrangements regarding business continuity plans).	Functional	Intersects With	Provider Contingency Plan	TPM-14.2	Mechanisms exist to contractually-require external service providers to have contingency plans that meet organizational contingency requirements.	3		BCD-10.3
3.7.3-86	N/A	Furthermore, as part of the response and recovery plans, a financial institution should consider and implement continuity measures to mitigate failures of third-party providers, which are of key importance for a financial institution's ICT service continuity (in line with the provisions of the Circular CSSF 22/806 on outsourcing arrangements regarding business continuity plans).	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-21	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5		TPM-11
3.7.4	Testing of Plans	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.7.4-87	N/A	Financial institutions should test their BCPs periodically. In particular, they should ensure that the BCPs of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually, in accordance with paragraph 89.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	8		BCD-04
3.7.4-87	N/A	Financial institutions should test their BCPs periodically. In particular, they should ensure that the BCPs of their critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually, in accordance with paragraph 89.	Functional	Intersects With	Coordinated Testing with Related Plans	BCD-10.1	Mechanisms exist to coordinate contingency plan testing with internal and external parties responsible for related plans.	3		BCD-04.1
3.7.4-88	N/A	BCPs should be updated at least annually, based on testing results, current threat intelligence and lessons learned from previous events. Any changes in recovery objectives (including RTOs and RPOs) and/or changes in business functions, supporting processes and information assets, should also be considered, where relevant, as a basis for updating the BCPs.	Functional	Intersects With	Ongoing Contingency Planning	BCD-07	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including third-party services); (3) Technologies (e.g., new, altered or decommissioned technologies); (4) Data (e.g., changes to data flows and/or data repositories); (5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or (6) Feedback from contingency plan testing	8		BCD-06
3.7.4-88	N/A	BCPs should be updated at least annually, based on testing results, current threat intelligence and lessons learned from previous events. Any changes in recovery objectives (including RTOs and RPOs) and/or changes in business functions, supporting processes and information assets, should also be considered, where relevant, as a basis for updating the BCPs.	Functional	Intersects With	Contingency Planning Components	BCD-07.1	Mechanisms exist to identify components that potentially impact the organization's ability to execute contingency plans, including changes to: (1) Personnel roles; (2) Business processes (including the use of third-party services); (3) Deployed technologies; (4) Data repositories and/or data flows; and/or (5) Physical infrastructure.	5		BCD-06.1
3.7.4-89	Financial institutions' testing of their BCPs should demonstrate that they are able to sustain the viability of their businesses until critical operations are re-established. In particular they should:	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.7.4-89.a	N/A	include testing of an adequate set of severe but plausible scenarios including those considered for the development of the BCPs (as well as testing of services provided by third parties, where applicable); this should include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that they can be run in this way for a sufficiently representative period of time and that normal functioning can be restored afterwards;	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
3.7.4-89.a	N/A	include testing of an adequate set of severe but plausible scenarios including those considered for the development of the BCPs (as well as testing of services provided by third parties, where applicable); this should include the switch-over of critical business functions, supporting processes and information assets to the disaster recovery environment and demonstrating that they can be run in this way for a sufficiently representative period of time and that normal functioning can be restored afterwards;	Functional	Intersects With	Contingency Plan Testing For Alternate Storage & Processing Sites	BCD-10.2	Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations.	5		BCD-04.2
3.7.4-89.b	N/A	be designed to challenge the assumptions on which BCPs rest, including governance arrangements and crisis communication plans; and	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04

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

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

Focal Document: **Commission de Surveillance du Secteur Financier (CSSF) Circular 20/750 - ICT Risk Management (2020)**
Focal Document URL: https://www.cssf.lu/en/document/circular-cssf-20-750/
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-lux-cssf-20-750.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.7.4-89.c	N/A	include procedures to verify the ability of their staff and contractors, ICT systems and ICT services to respond adequately to the scenarios defined in paragraph 89(a).	Functional	Intersects With	Contingency Training	BCD-09	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	3		BCD-03
3.7.4-89.c	N/A	include procedures to verify the ability of their staff and contractors, ICT systems and ICT services to respond adequately to the scenarios defined in paragraph 89(a).	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
3.7.4-90	N/A	Test results should be documented and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the management body.	Functional	Intersects With	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-11	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5		BCD-05
3.7.4-90	N/A	Test results should be documented and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the management body.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3		GOV-01.2
3.7.4-90	N/A	Test results should be documented and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the management body.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and (11) Disposition statement (e.g., closeout summary).	3		IAO-05
3.7.5	Crisis Communication	N/A	Functional	No Relationship	N/A	N/A	N/A	0		
3.7.5-91	N/A	In the event of a disruption or emergency, and during the implementation of the BCPs, financial institutions should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the competent authorities when required by national regulations, and also relevant providers (outsourcing providers, group entities, or third-party providers) are informed in a timely and appropriate manner.	Functional	Intersects With	Recovery Operations Communications	BCD-06	Mechanisms exist to communicate the status of recovery activities and progress in restoring operational capabilities to designated internal and external stakeholders.	8		BCD-01.6
3.7.5-91	N/A	In the event of a disruption or emergency, and during the implementation of the BCPs, financial institutions should ensure that they have effective crisis communication measures in place so that all relevant internal and external stakeholders, including the competent authorities when required by national regulations, and also relevant providers (outsourcing providers, group entities, or third-party providers) are informed in a timely and appropriate manner.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10