**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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Title I | General Principle | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 1 | Overall risk profile and complexity | For the purposes of defining and implementing ICT risk management tools, methods, processes, policies and procedures referred to in Title II and the simplified ICT risk management framework referred to in Title III, elements of increased or reduced complexity or the overall risk profile shall be taken into account, including elements relating to encryption and cryptography, ICT operations security, network security, ICT project and change management and the potential impact of the ICT risk on confidentiality, integrity and availability of data, and of the disruptions on the continuity and availability of the financial entity's | Functional | Intersects With | Defining Business Context & Mission | GOV-06 | Mechanisms exist to document the organization's business model and mission. | 3 | | GOV-08 |
| Article 1 | Overall risk profile and complexity | For the purposes of defining and implementing ICT risk management tools, methods, processes, policies and procedures referred to in Title II and the simplified ICT risk management framework referred to in Title III, elements of increased or reduced complexity or the overall risk profile shall be taken into account, including elements relating to encryption and cryptography, ICT operations security, network security, ICT project and change management and the potential impact of the ICT risk on confidentiality, integrity and availability of data, and of the disruptions on the continuity and availability of the financial entity's | 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:<br>(1) The organization's Enterprise Risk Management (ERM); and<br>(2) Industry-recognized cybersecurity risk management practices. | 3 | | RSK-01 |
| Title II | Further Harmonisation of ICT Risk Management Tools, Methods, Processes and Policies in Accordance with Article 15 of Regulation (EU) | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Title II - Chapter I | ICT Security Policies, Procedures, Protocols, and Tools | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Title II - Chapter I - Section I | N/A | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 2.1 | General elements of ICT security policies | Financial entities shall ensure that their ICT security policies concerning information security and related procedures, protocols and tools are embedded in the ICT risk management framework. Financial entities shall establish the ICT security policies, procedures, protocols and tools referred to in this Chapter with a view to ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse, preserving the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guaranteeing an accurate and prompt data transmission without major disruptions and undue delays. | 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 |
| Article 2.1 | General elements of ICT security policies | Financial entities shall ensure that their ICT security policies concerning information security and related procedures, protocols and tools are embedded in the ICT risk management framework. Financial entities shall establish the ICT security policies, procedures, protocols and tools referred to in this Chapter with a view to ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse, preserving the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guaranteeing an accurate and prompt data transmission without major disruptions and undue delays. | 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:<br>(1) The organization's Enterprise Risk Management (ERM); and<br>(2) Industry-recognized cybersecurity risk management practices. | 3 | | RSK-01 |
| Article 2.2 | General elements of ICT security policies | Financial entities shall ensure that the ICT security policies referred to in paragraph 1: | 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 |
| Article 2.2(a) | General elements of ICT security policies | are aligned to the financial entity's information security objectives included in the digital operational resilience strategy referred to in Article 6(8) of Regulation (EU) 2022/2554; | Functional | Intersects With | Strategic Plan & Objectives | PRM-02 | Mechanisms exist to establish a:<br>(1) Strategic security, compliance and resilience-specific business plan; and<br>(2) Set of objectives to achieve that plan. | 5 | | PRM-01.1 |
| Article 2.2(b) | General elements of ICT security policies | indicate the date of formal approval 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. | 3 | | GOV-02 |
| Article 2.2(c) | General elements of ICT security policies | include indicators and measures to monitor the implementation of the ICT security policies and to record exceptions from the implementation of these policies. In case of exceptions, the digital operational resilience of the financial entity shall be ensured; | Functional | Intersects With | Exception Management | GOV-04.2 | Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded. | 5 | | GOV-02.1 |
| Article 2.2(c) | General elements of ICT security policies | include indicators and measures to monitor the implementation of the ICT security policies and to record exceptions from the implementation of these policies. In case of exceptions, the digital operational resilience of the financial entity shall be ensured; | Functional | Intersects With | Measures of Performance | GOV-12 | Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance. | 5 | | GOV-05 |
| Article 2.2(d) | General elements of ICT security policies | set out the responsibilities of staff at all levels to ensure the financial entity's ICT security; | 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 |
| Article 2.2(d) | General elements of ICT security policies | set out the responsibilities of staff at all levels to ensure the financial entity's ICT security; | Functional | Intersects With | Defined Roles & Responsibilities | HRS-04 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | | HRS-03 |
| Article 2.2(e) | General elements of ICT security policies | set out the consequences of non-compliance with the ICT security policies from staff of the financial entity, where such provisions on the consequence of non-compliance with policies of the financial entity are not included in other policies of the financial entity; | Functional | Intersects With | Personnel Sanctions | HRS-10 | Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures. | 8 | | HRS-07 |
| Article 2.2(f) | General elements of ICT security policies | list the documentation to be maintained; | 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 |
| Article 2.2(g) | General elements of ICT security policies | specify the segregation of duties' arrangements to avoid conflicts of interest, in the context of the three lines of defence model or other internal risk management and control model, as applicable; | Functional | Intersects With | Separation of Duties (SoD) | HRS-14 | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion. | 8 | | HRS-11 |
| Article 2.2(h) | General elements of ICT security policies | consider leading practices and, where applicable, standards as defined in Article 2, point (1), of Regulation (EU) No 1025/2012; | Functional | Intersects With | Secure Practices Alignment Justification | GOV-03.1 | Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that:<br>(1) Support external scrutiny; and<br>(2) Provide defensible justification for secure | 5 | | GOV-01.4 |
| Article 2.2(h) | General elements of ICT security policies | consider leading practices and, where applicable, standards as defined in Article 2, point (1), of Regulation (EU) No 1025/2012; | Functional | Intersects With | Secure Engineering Principles | SEA-05 | Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS). | 3 | | SEA-01 |
| Article 2.2(i) | General elements of ICT security policies | identify the roles and responsibilities for the ICT security policies' development, implementation and maintenance; | 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 |
| Article 2.2(j) | General elements of ICT security policies | are reviewed in accordance with the requirements set out in in Article 6(5) of Regulation (EU) 2022/2554; | 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 |
| Article 2.2(k) | General elements of ICT security policies | take into account material changes concerning the financial entity, including material changes to the activities or processes of the financial entity, or to the cyber threat landscape or to the applicable legal obligations. | 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 |

**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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 2.2(k) | General elements of ICT security policies | take into account material changes concerning the financial entity, including material changes to the activities or processes of the financial entity, or to the cyber threat landscape or to the applicable legal obligations. | 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 |
| Title II - Chapter I - Section II | N/A | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 3.1 | ICT risk management | Financial entities shall develop, document and implement policies and procedures concerning ICT risk management that are necessary to ensure the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delay. The policies and procedures concerning ICT risk management shall include all of the | 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:<br>(1) The organization's Enterprise Risk Management (ERM); and<br>(2) Industry-recognized cybersecurity risk management practices. | 10 | | RSK-01 |
| Article 3.1(a) | ICT risk management | the indication of the approval of the risk tolerance level for ICT risk established according to Article 6(8), point (b), of Regulation (EU) 2022/2554; | Functional | Intersects With | Risk Tolerance | RSK-05.1 | Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results. | 8 | | RSK-01.3 |
| Article 3.1(b) | ICT risk management | the procedure and the methodology to conduct the ICT risk assessment, identifying vulnerabilities and threats that affect or may affect the supported business functions, the ICT systems and ICT assets supporting those functions and the quantitative or qualitative indicators to measure impact and likelihood of those vulnerabilities being exploited by threats; | Functional | Intersects With | Risk Identification | RSK-09 | Mechanisms exist to identify and document risks, both internal and external. | 3 | | RSK-03 |
| Article 3.1(b) | ICT risk management | the procedure and the methodology to conduct the ICT risk assessment, identifying vulnerabilities and threats that affect or may affect the supported business functions, the ICT systems and ICT assets supporting those functions and the quantitative or qualitative indicators to measure impact and likelihood of those vulnerabilities being exploited by threats; | Functional | Intersects With | Risk Assessment Methodology | RSK-12 | Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations. | 8 | | RSK-04.2 |
| Article 3.1(b) | ICT risk management | the procedure and the methodology to conduct the ICT risk assessment, identifying vulnerabilities and threats that affect or may affect the supported business functions, the ICT systems and ICT assets supporting those functions and the quantitative or qualitative indicators to measure impact and likelihood of those vulnerabilities being exploited by threats; | 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 |
| Article 3.1(c) | ICT risk management | the procedure to identify, implement and document ICT risk treatment measures for the ICT risk assessed, including the determination of ICT risk treatment measures necessary to bring ICT risk within the risk tolerance levels referred to in point (a). The procedure shall ensure the monitoring of the effectiveness of the measures implemented, the assessment of whether the established risk tolerance levels of the financial entity have been attained and that the financial entity takes actions to correct or improve the measures where necessary; | Functional | Intersects With | Risk Remediation | RSK-17 | Mechanisms exist to remediate risks to an acceptable level. | 8 | | RSK-06 |
| Article 3.1(c) | ICT risk management | the procedure to identify, implement and document ICT risk treatment measures for the ICT risk assessed, including the determination of ICT risk treatment measures necessary to bring ICT risk within the risk tolerance levels referred to in point (a). The procedure shall ensure the monitoring of the effectiveness of the measures implemented, the assessment of whether the established risk tolerance levels of the financial entity have been attained and that the financial entity takes actions to correct or improve 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:<br>(1) The effectiveness of security, compliance and resilience controls;<br>(2) Changes to the organization's risk profile; and<br>(3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk. | 5 | | RSK-11 |
| Article 3.1(d) | ICT risk management | with reference to the ICT risk that is still present following the implementation of the ICT risk treatment measures: | Functional | Intersects With | Risk Treatment Options | RSK-16.1 | Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including:<br>(1) Mitigating the risk to an acceptable level;<br>(2) Avoiding the risk (e.g., terminating the project);<br>(3) Transferring the risk to a third party (e.g., insurance and service provider); or<br>(4) Accepting the risk. | 5 | | RSK-06.3 |
| Article 3.1(d)(i) | ICT risk management | provisions on the identification of residual ICT risks; | 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 |
| Article 3.1(d)(i) | ICT risk management | provisions on the identification of residual ICT risks; | Functional | Intersects With | Risk Treatment Options | RSK-16.1 | Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including:<br>(1) Mitigating the risk to an acceptable level;<br>(2) Avoiding the risk (e.g., terminating the project);<br>(3) Transferring the risk to a third party (e.g., insurance and service provider); or<br>(4) Accepting the risk. | 3 | | RSK-06.3 |
| Article 3.1(d)(ii) | ICT risk management | the assignment of roles and responsibilities regarding the acceptance of the residual ICT risks that exceed the financial entity's risk tolerance level referred to in point (a), and for the assessment process referred to in point (iv); | Functional | Intersects With | Executive Leadership Approval For Managing Material Risk | RSK-06.1 | Mechanisms exist to obtain executive leadership approval for risk management decisions involving material risk. | 5 | | RSK-13 |
| Article 3.1(d)(ii) | ICT risk management | the assignment of roles and responsibilities regarding the acceptance of the residual ICT risks that exceed the financial entity's risk tolerance level referred to in point (a), and for the assessment process referred to in point (iv); | Functional | Intersects With | Risk Owner | RSK-11 | Mechanisms exist to identify a risk owner for each item in the risk register to ensure clear accountability for unremediated risks. | 3 | | RSK-03.2 |
| Article 3.1(d)(iii) | ICT risk management | the development of an inventory of the accepted residual ICT risks, including an explanation of the reasons for which they were accepted; | Functional | Intersects With | Documented Justification For Material Risk Management | RSK-06.2 | Mechanisms exist to document executive leadership justification for selecting a specific course of action to manage material risk. | 5 | | RSK-13.2 |
| Article 3.1(d)(iii) | ICT risk management | the development of an inventory of the accepted residual ICT risks, including an explanation of the reasons for which they were accepted; | Functional | Intersects With | Risk Register | RSK-14 | Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks. | 5 | | RSK-04.1 |
| Article 3.1(d)(iv) | ICT risk management | provisions on the assessment of the accepted residual ICT risks at least once a year, including the identification of any changes to the residual ICT risks, the assessment of available mitigation measures and the assessment of whether the reasons justifying the acceptance of residual ICT risks are still valid and applicable at the date of the | 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 |
| Article 3.1(d)(iv) | ICT risk management | provisions on the assessment of the accepted residual ICT risks at least once a year, including the identification of any changes to the residual ICT risks, the assessment of available mitigation measures and the assessment of whether the reasons justifying the acceptance of residual ICT risks are still valid and applicable at the date of the | Functional | Intersects With | Risk Register | RSK-14 | Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks. | 3 | | RSK-04.1 |
| Article 3.1(e) | ICT risk management | provisions on the monitoring of any changes to the ICT risk and cyber threat landscape, internal and external vulnerabilities and threats and of ICT risk of the financial entity to promptly detect changes that could affect its ICT risk profile; | Functional | Intersects With | Risk Monitoring | RSK-22 | Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including:<br>(1) The effectiveness of security, compliance and resilience controls;<br>(2) Changes to the organization's risk profile; and<br>(3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk. | 5 | | RSK-11 |
| Article 3.1(e) | ICT risk management | provisions on the monitoring of any changes to the ICT risk and cyber threat landscape, internal and external vulnerabilities and threats and of ICT risk of the financial entity to promptly detect changes that could affect its ICT risk profile; | 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 |
| Article 3.1(e) | ICT risk management | provisions on the monitoring of any changes to the ICT risk and cyber threat landscape, internal and external vulnerabilities and threats and of ICT risk of the financial entity to promptly detect changes that could affect its ICT risk profile; | Functional | Intersects With | Vulnerability & Patch Management Program (VPMP) | VPM-02 | Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities. | 3 | | VPM-01 |

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

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

Focal Document: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 3.1(f) | ICT risk management | provisions on a process to ensure that changes to the business strategy and the digital operational resilience strategy of the financial entity, if any, are taken into account. | Functional | Intersects With | Periodic Review & Update of Security, Compliance & Resilience Program | GOV-04.1 | Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and | 3 | | GOV-03 |
| Article 3.1(f) | ICT risk management | provisions on a process to ensure that changes to the business strategy and the digital operational resilience strategy of the financial entity, if any, are taken into account. | Functional | Intersects With | Strategic Plan & Objectives | PRM-02 | Mechanisms exist to establish a:<br>(1) Strategic security, compliance and resilience-specific business plan; and<br>(2) Set of objectives to achieve that plan. | 5 | | PRM-01.1 |
| Title II - Chapter I - Section III | ICT Asset Management | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 4.1 | ICT asset management policy | As part of the ICT security policies, financial entities shall develop, document and implement a policy on management of ICT assets necessary to preserve the availability, authenticity, integrity and confidentiality of data. | Functional | Subset Of | Asset Management Policy | AST-01 | Mechanisms exist to establish a formal, documented asset management policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected | 10 | | |
| Article 4.1 | ICT asset management policy | As part of the ICT security policies, financial entities shall develop, document and implement a policy on management of ICT assets necessary to preserve the availability, authenticity, integrity and confidentiality of data. | Functional | Intersects With | Asset Governance | AST-02 | Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls. | 8 | | AST-01 |
| Article 4.2 | ICT asset management policy | The policy on management of ICT assets shall: | Functional | Subset Of | Asset Management Policy | AST-01 | Mechanisms exist to establish a formal, documented asset management policy that:<br>(1) Conveys executive management's intent; | 10 | | |
| Article 4.2 | ICT asset management policy | The policy on management of ICT assets shall: | Functional | Intersects With | Asset Governance | AST-02 | Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls. | 5 | | AST-01 |
| Article 4.2(a) | ICT asset management policy | require the monitoring and management of the life cycle of ICT assets identified and classified in accordance with Article 8(1) of Regulation (EU) 2022/2554; | Functional | Intersects With | Asset Governance | AST-02 | Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls. | 3 | | AST-01 |
| Article 4.2(a) | ICT asset management policy | require the monitoring and management of the life cycle of ICT assets identified and classified in accordance with Article 8(1) of Regulation (EU) 2022/2554; | 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 |
| Article 4.2(b) | ICT asset management policy | require the financial entity to keep records of all of the following: | Functional | Intersects With | Asset Inventories | AST-04 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel. | 8 | | AST-02 |
| Article 4.2(b)(i) | ICT asset management policy | unique identifier of each ICT asset; | Functional | Intersects With | Asset Inventories | AST-04 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel. | 5 | | AST-02 |
| Article 4.2(b)(ii) | ICT asset management policy | information on the location, either physical or logical, of all ICT assets; | Functional | Intersects With | Asset Inventories | AST-04 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel. | 5 | | AST-02 |
| Article 4.2(b)(iii) | ICT asset management policy | the classification of all ICT assets, as specified in Article 8(1) of Regulation (EU) 2022/2254; | Functional | Intersects With | Asset Categorization | AST-15 | Mechanisms exist to categorize Technology Assets, Applications and/or Services (TAAS). | 5 | | AST-31 |
| Article 4.2(b)(iii) | ICT asset management policy | the classification of all ICT assets, as specified in Article 8(1) of Regulation (EU) 2022/2254; | Functional | Intersects With | Data & Asset Classification | DCH-04 | Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements. | 3 | | DCH-02 |
| Article 4.2(b)(iv) | ICT asset management policy | the identity of ICT asset owners; | 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. | 8 | | AST-03 |
| Article 4.2(b)(v) | ICT asset management policy | business functions or services supported by the ICT asset; | 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 |
| Article 4.2(b)(vi) | ICT asset management policy | the ICT business continuity requirements, including recovery time objectives and recovery point objective; | Functional | Intersects With | Identify Critical Assets | AST-05 | Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions. | 3 | | BCD-02 |
| Article 4.2(b)(vi) | ICT asset management policy | the ICT business continuity requirements, including recovery time objectives and recovery point objective; | Functional | Intersects With | Recovery Time / Point Objectives (RTO / RPO) | BCD-04.1 | Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 5 | | BCD-01.4 |
| Article 4.2(b)(vii) | ICT asset management policy | whether the ICT asset may be or is exposed to external networks, including the internet; | Functional | Intersects With | Asset Inventories | AST-04 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel. | 3 | | AST-02 |
| Article 4.2(b)(viii) | ICT asset management policy | the links and interdependencies among ICT assets and the business functions using each ICT asset; | 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 |

**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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 4.2(b)(viii) | ICT asset management policy | the links and interdependencies among ICT assets and the business functions using each ICT asset; | Functional | Intersects With | Network Diagrams & Data Flow Diagrams (DFDs) | AST-17 | Mechanisms exist to maintain network architecture diagrams that:<br>(1) Contain sufficient detail to assess the security of the network's architecture;<br>(2) Reflect the current architecture of the network environment; and<br>(3) Document all sensitive and/or regulated data flows. | 3 | | AST-04 |
| Article 4.2(b)(ix) | ICT asset management policy | where applicable, for all ICT assets, the end dates of the ICT third-party service provider's regular, extended and custom support services after which it is no longer supported by its supplier or by an ICT third-party service provider; | 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 |
| Article 4.2(b)(ix) | ICT asset management policy | where applicable, for all ICT assets, the end dates of the ICT third-party service provider's regular, extended and custom support services after which it is no longer supported by its supplier or by an ICT third-party service provider; | 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:<br>(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and<br>(2) Requiring justification and documented approval for the continued use of unsupported TAAS required | 5 | | TDA-17 |
| Article 4.2(c) | ICT asset management policy | for financial entities referred to in Article 8(7) of Regulation (EU) 2022/2554, prescribe that they keep records of the information needed to perform a specific ICT risk assessment on all legacy ICT systems. | 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 |
| Article 4.2(c) | ICT asset management policy | for financial entities referred to in Article 8(7) of Regulation (EU) 2022/2554, prescribe that they keep records of the information needed to perform a specific ICT risk assessment on all legacy ICT systems. | 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 |
| Article 5.1 | ICT asset management procedure | Financial entities shall develop, document and implement an ICT asset management procedure, with a view to preserving the availability, authenticity, integrity and confidentiality of data. | Functional | Intersects With | Asset Governance | AST-02 | Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls. | 5 | | AST-01 |
| Article 5.2 | ICT asset management procedure | Such procedure shall detail the criteria to perform the criticality assessment of information assets and ICT assets supporting business functions. The assessment shall take into account the ICT risk related to those business functions and their dependencies on the information assets or ICT assets and how the loss of confidentiality, integrity, availability of such information assets and ICT assets would impact their business processes and activities of the financial entity. | 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 |
| Article 5.2 | ICT asset management procedure | Such procedure shall detail the criteria to perform the criticality assessment of information assets and ICT assets supporting business functions. The assessment shall take into account the ICT risk related to those business functions and their dependencies on the information assets or ICT assets and how the loss of confidentiality, integrity, availability of such information assets and ICT assets would impact their business processes and activities of the financial entity. | 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:<br>(1) Document the security categorization results (including supporting rationale) in the security plan for systems; and<br>(2) Ensure the security categorization decision is reviewed and approved by the asset owner. | 5 | | RSK-02 |
| Title II - Chapter I - Section IV | Encryption and Cryptography | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 6.1 | Encryption and cryptographic controls | As part of their ICT security policies, financial entities shall develop, document and implement a policy on encryption and cryptographic controls, with a view to preserve the availability, authenticity, integrity and confidentiality of data. | Functional | Intersects With | Use of Cryptographic Controls | CRY-02 | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies. | 8 | | CRY-01 |
| Article 6.2 | Encryption and cryptographic controls | The policy on encryption and cryptographic controls shall be designed on the basis of the results of approved data classification and ICT risk assessment and shall include all the following elements: | Functional | Intersects With | Use of Cryptographic Controls | CRY-02 | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic | 5 | | CRY-01 |
| Article 6.2(a) | Encryption and cryptographic controls | rules for the encryption of data at rest and in transit; | Functional | Intersects With | Encrypting Data In Transit | CRY-05 | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit. | 5 | | CRY-03 |
| Article 6.2(a) | Encryption and cryptographic controls | rules for the encryption of data at rest and in transit; | Functional | Intersects With | Encrypting Data At Rest | CRY-07 | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest. | 5 | | CRY-05 |
| Article 6.2(b) | Encryption and cryptographic controls | rules for the encryption of data in use, where necessary. Where encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment or take other equivalent measures that ensure the confidentiality, integrity, authenticity and availability of data; | Functional | Intersects With | Use of Cryptographic Controls | CRY-02 | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies. | 3 | | CRY-01 |
| Article 6.2(b) | Encryption and cryptographic controls | rules for the encryption of data in use, where necessary. Where encryption of data in use is not possible, financial entities shall process data in use in a separated and protected environment or take other equivalent measures that ensure the confidentiality, integrity, authenticity and availability of data; | Functional | Intersects With | Process Isolation | SEA-09 | Mechanisms exist to implement a separate execution domain for each executing process. | 3 | | SEA-04 |
| Article 6.2(c) | Encryption and cryptographic controls | rules for the encryption of internal network connections and traffic with external parties; | Functional | Intersects With | Encrypting Data In Transit | CRY-05 | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit. | 5 | | CRY-03 |
| Article 6.2(d) | Encryption and cryptographic controls | provisions for cryptographic key management establishing the correct use, protection and lifecycle of cryptographic keys in accordance with Article 7. | Functional | Intersects With | Cryptographic Key Management | CRY-10 | Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys. | 8 | | CRY-09 |
| Article 6.3 | Encryption and cryptographic controls | Financial entities shall include in the policy on encryption and cryptographic controls criteria to select cryptographic techniques and use practices taking into account leading practices and standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012, and the classification of relevant ICT assets established according to Article 8(1) of Regulation (EU) 2022/2554. Where the financial entity cannot adhere to the leading practices or use the most reliable techniques, it shall adopt mitigation and monitoring measures to ensure resiliency against cyber threats. | Functional | Intersects With | Use of Cryptographic Controls | CRY-02 | Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies. | 5 | | CRY-01 |
| Article 6.4 | Encryption and cryptographic controls | Financial entities shall include in the policy on encryption and cryptographic controls provisions to, where necessary, on the basis of developments in cryptanalysis, update or change the cryptographic technology to ensure they remain resilient against cyber threats and considering the information resources referred to in Article 10(2), point (a). Where the financial entity cannot update or change the cryptographic technology, it shall adopt mitigation and monitoring measures to ensure they remain resilient against cyber threats. | Functional | Intersects With | Cryptographic Agility Risk Assessment (CARA) | QTS-04 | Mechanisms exist to perform a Cryptographic Agility Risk Assessment (CARA) that analyzes Technology Assets, Applications, Services and Data (TAASD) to:<br>(1) Identify TAASD most vulnerable to quantum-enabled cryptanalytic threats; and<br>(2) Prioritize TAASD based on potential business impact. | 5 | | QTS-02 |
| Article 6.4 | Encryption and cryptographic controls | Financial entities shall include in the policy on encryption and cryptographic controls provisions to, where necessary, on the basis of developments in cryptanalysis, update or change the cryptographic technology to ensure they remain resilient against cyber threats and considering the information resources referred to in Article 10(2), point (a). Where the financial entity cannot update or change the cryptographic technology, it shall adopt mitigation and monitoring measures to ensure they remain resilient against cyber threats. | Functional | Intersects With | Deprecated Cryptographic Algorithms | QTS-09.5 | Mechanisms exist to identify and disallow quantum-vulnerable and otherwise deprecated cryptographic algorithms. | 5 | | QTS-06.5 |
| Article 6.5 | Encryption and cryptographic controls | Financial entities shall include a requirement in the policy on encryption and cryptographic controls to record the adoption of mitigation and monitoring measures adopted in accordance with paragraphs 3 and 4 and to provide a reasoned explanation for doing so. | Functional | Intersects With | Exception Management | GOV-04.2 | Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded. | 5 | | GOV-02.1 |
| Article 7.1 | Cryptographic key management | Financial entities shall lay out in the provisions on cryptographic key management referred to in Article 6(2) point (d), the requirements for managing cryptographic keys through their whole lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking and destroying keys. | Functional | Intersects With | Cryptographic Key Management | CRY-10 | Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys. | 8 | | CRY-09 |
| Article 7.2 | Cryptographic key management | Financial entities shall identify and implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure and modification. The controls shall be designed taking into account the results of the approved data classification and the ICT risk assessment processes. | Functional | Intersects With | Cryptographic Key Management | CRY-10 | Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys. | 5 | | CRY-09 |

**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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 7.2 | Cryptographic key management | Financial entities shall identify and implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure and modification. The controls shall be designed taking into account the results of the approved data classification and the ICT risk assessment processes. | Functional | Intersects With | Control & Distribution of Cryptographic Keys | CRY-10.4 | Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes. | 5 | | CRY-09.4 |
| Article 7.3 | Cryptographic key management | Financial entities shall develop and implement methods to replace the cryptographic keys in the case of lost, compromised or damaged keys. | Functional | Intersects With | Cryptographic Key Loss or Change | CRY-10.3 | Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users. | 8 | | CRY-09.3 |
| Article 7.4 | Cryptographic key management | Financial entities shall create and maintain a register for all certificates and certificate- storing devices for at least ICT assets supporting critical or important functions. The register shall be kept up-to-date. | Functional | Intersects With | Asset Inventories | AST-04 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel. | 3 | | AST-02 |
| Article 7.4 | Cryptographic key management | Financial entities shall create and maintain a register for all certificates and certificate- storing devices for at least ICT assets supporting critical or important functions. The register shall be kept up-to-date. | Functional | Intersects With | Certificate Monitoring | CRY-13 | Automated mechanisms exist to discover when new certificates are issued for organization-controlled domains. | 5 | | CRY-12 |
| Article 7.5 | Cryptographic key management | Financial entities shall ensure the prompt renewal of certificates in advance of their expiration. | Functional | Intersects With | Public Key Infrastructure (PKI) | CRY-09 | Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service | 3 | | CRY-08 |
| Article 7.5 | Cryptographic key management | Financial entities shall ensure the prompt renewal of certificates in advance of their expiration. | Functional | Intersects With | Certificate Monitoring | CRY-13 | Automated mechanisms exist to discover when new certificates are issued for organization-controlled domains. | 5 | | CRY-12 |
| Title II - Chapter I - Section V | ICT Operations Security | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 8.1 | Policies and procedures for ICT operations | As part of the ICT security policies and procedures, financial entities shall develop, document and implement policies and procedures to manage the ICT operations of ICT assets, with a view to ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse and preserving the availability, authenticity, integrity and confidentiality of data. These policies and procedures shall define how financial entities operate, monitor, control and restore their ICT assets, including the documentation of ICT operations. | Functional | Intersects With | Operations Security | OPS-02 | Mechanisms exist to facilitate the implementation of operational security controls. | 5 | | OPS-01 |
| Article 8.1 | Policies and procedures for ICT operations | As part of the ICT security policies and procedures, financial entities shall develop, document and implement policies and procedures to manage the ICT operations of ICT assets, with a view to ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse and preserving the availability, authenticity, integrity and confidentiality of data. These policies and procedures shall define how financial entities operate, monitor, control and restore their ICT assets, including the documentation of ICT operations. | 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 |
| Article 8.2 | Policies and procedures for ICT operations | The policies and procedures for ICT operations referred to in paragraph 1 shall include all of the following elements: | 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 |
| Article 8.2(a) | Policies and procedures for ICT operations | ICT assets description, including all of the following: | 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. | 3 | | OPS-01.1 |
| Article 8.2(a)(i) | Policies and procedures for ICT operations | secure installation, maintenance, configuration and deinstallation of ICT systems; | Functional | Intersects With | Secure Baseline Configurations | CFG-04 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards. | 5 | | CFG-02 |
| Article 8.2(a)(i) | Policies and procedures for ICT operations | secure installation, maintenance, configuration and deinstallation of ICT systems; | Functional | Intersects With | Maintenance Operations | MNT-02 | Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise. | 3 | | MNT-01 |
| Article 8.2(a)(ii) | Policies and procedures for ICT operations | management of information assets used by ICT assets, including their processing and handling, automated and manual; | Functional | Intersects With | Data Protection | DCH-02 | Mechanisms exist to facilitate the implementation of data protection controls. | 5 | | DCH-01 |
| Article 8.2(a)(iii) | Policies and procedures for ICT operations | identification and control of legacy ICT systems; | 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 |
| Article 8.2(a)(iii) | Policies and procedures for ICT operations | identification and control of legacy ICT systems; | 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:<br>(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and<br>(2) Requiring justification and documented approval for the continued use of unsupported TAAS required | 5 | | TDA-17 |
| Article 8.2(b) | Policies and procedures for ICT operations | controls and monitoring of ICT systems, including all of the following: | 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. | 3 | | OPS-01.1 |
| Article 8.2(b)(i) | Policies and procedures for ICT operations | backup and restoration requirements of ICT systems; | 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 |
| Article 8.2(b)(ii) | Policies and procedures for ICT operations | scheduling requirements, taking into consideration interdependencies among the ICT systems; | 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. | 3 | | OPS-01.1 |
| Article 8.2(b)(iii) | Policies and procedures for ICT operations | protocols for audit-trail and system log information; | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5 | | MON-03 |
| Article 8.2(b)(iii) | Policies and procedures for ICT operations | protocols for audit-trail and system log information; | Functional | Intersects With | Event Log & Security-Relevant Telemetry Retention | MON-13 | Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements. | 3 | | MON-10 |
| Article 8.2(b)(iv) | Policies and procedures for ICT operations | requirements to ensure that the performance of internal audit and other testing minimises disruptions to business operations; | 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. | 8 | | CPL-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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 8.2(b)(v) | Policies and procedures for ICT operations | requirements on the separation of ICT production environments from the development, testing and other non-production environments. The separation shall consider all of the components of the environment, such as accounts, data or connections; | 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 |
| Article 8.2(b)(vi) | Policies and procedures for ICT operations | requirements to conduct the development and testing in environments which are separated from the production environment; | 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 |
| Article 8.2(b)(vii) | Policies and procedures for ICT operations | requirements to conduct the development and testing in production environments. The policies and procedures shall provide that the instances in which testing is performed in production environment are clearly identified, justified, for limited periods of time approved by the relevant function, and considering Article 16(6). The availability, confidentiality, integrity and authenticity of ICT systems and production data shall be ensured during development and test activities in production environment; | 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). | 5 | | TDA-08 |
| Article 8.2(b)(vii) | Policies and procedures for ICT operations | requirements to conduct the development and testing in production environments. The policies and procedures shall provide that the instances in which testing is performed in production environment are clearly identified, justified, for limited periods of time approved by the relevant function, and considering Article 16(6). The availability, confidentiality, integrity and authenticity of ICT systems and production data shall be ensured during development and test activities in production environment; | 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 |
| Article 8.2(c) | Policies and procedures for ICT operations | error handling concerning ICT systems, including all of the following: | Functional | Intersects With | Error Handling | TDA-12.1 | Mechanisms exist to handle error conditions by:<br>(1) Identifying potentially security-relevant error conditions;<br>(2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and<br>(3) Revealing error messages only to authorized personnel. | 3 | | TDA-19 |
| Article 8.2(c)(i) | Policies and procedures for ICT operations | procedures and protocols for handling errors; | Functional | Intersects With | Error Handling | TDA-12.1 | Mechanisms exist to handle error conditions by:<br>(1) Identifying potentially security-relevant error conditions;<br>(2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and<br>(3) Revealing error messages only to authorized personnel. | 3 | | TDA-19 |
| Article 8.2(c)(ii) | Policies and procedures for ICT operations | support and escalation contacts, including external support contacts in case of unexpected operational or technical issues; | 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. | 3 | | OPS-01.1 |
| Article 8.2(c)(iii) | Policies and procedures for ICT operations | ICT system restart, rollback and recovery procedures for use in the event of ICT system disruption. | Functional | Intersects With | Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | BCD-18 | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure. | 5 | | BCD-12 |
| Article 9.1 | Capacity and performance management | As part of the ICT security procedures financial entities shall develop, document and implement capacity and performance management procedures to identify capacity requirements of their ICT systems and apply resource optimisation and monitoring procedures to maintain and improve the availability of data and ICT systems and efficiency of ICT systems and prevent ICT capacity shortages. | Functional | Intersects With | Capacity & Performance Planning Policy | CAP-01 | Mechanisms exist to establish a formal, documented capacity and performance planning policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors;<br>(3) Is reviewed at least annually; and | 5 | | |
| Article 9.1 | Capacity and performance management | As part of the ICT security procedures financial entities shall develop, document and implement capacity and performance management procedures to identify capacity requirements of their ICT systems and apply resource optimisation and monitoring procedures to maintain and improve the availability of data and ICT systems and efficiency of ICT systems and prevent ICT capacity shortages. | 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 |
| Article 9.1 | Capacity and performance management | As part of the ICT security procedures financial entities shall develop, document and implement capacity and performance management procedures to identify capacity requirements of their ICT systems and apply resource optimisation and monitoring procedures to maintain and improve the availability of data and ICT systems and efficiency of ICT systems and prevent ICT capacity shortages. | 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 |
| Article 9.1 | Capacity and performance management | As part of the ICT security procedures financial entities shall develop, document and implement capacity and performance management procedures to identify capacity requirements of their ICT systems and apply resource optimisation and monitoring procedures to maintain and improve the availability of data and ICT systems and efficiency of ICT systems and prevent ICT capacity shortages. | 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. | 8 | | OPS-01.1 |
| Article 9.2 | Capacity and performance management | The capacity and performance management procedures shall ensure that appropriate measures are taken to cater for the specificities of ICT systems with long or complex procurement or approval processes or that are resource-intensive. | 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 |
| Article 9.2 | Capacity and performance management | The capacity and performance management procedures shall ensure that appropriate measures are taken to cater for the specificities of ICT systems with long or complex procurement or approval processes or that are resource-intensive. | 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 |
| Article 10.1 | Vulnerability and patch management | As part of the ICT security procedures, financial entities shall develop, document and implement vulnerability management procedures with a view to ensuring the security of networks against intrusions and data misuse in order to preserve the availability, authenticity, integrity and confidentiality of data. | 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. | 8 | | OPS-01.1 |
| Article 10.1 | Vulnerability and patch management | As part of the ICT security procedures, financial entities shall develop, document and implement vulnerability management procedures with a view to ensuring the security of networks against intrusions and data misuse in order to preserve the availability, authenticity, integrity and confidentiality of data. | Functional | Intersects With | Vulnerability & Patch Management Policy | VPM-01 | Mechanisms exist to establish a formal, documented vulnerability and patch management policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors;<br>(3) Is reviewed at least annually; and<br>(4) Is updated, as necessary, to adapt to evolving | 5 | | |
| Article 10.1 | Vulnerability and patch management | As part of the ICT security procedures, financial entities shall develop, document and implement vulnerability management procedures with a view to ensuring the security of networks against intrusions and data misuse in order to preserve the availability, authenticity, integrity and confidentiality of data. | Functional | Intersects With | Vulnerability & Patch Management Program (VPMP) | VPM-02 | Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities. | 8 | | VPM-01 |
| Article 10.2 | Vulnerability and patch management | The vulnerability management procedures referred to in paragraph 1 shall: | 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 |
| Article 10.2(a) | Vulnerability and patch management | identify and update relevant and trustworthy information resources to build and maintain awareness about vulnerabilities; | Functional | Intersects With | Threat Intelligence Feeds | THR-04 | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 5 | | THR-03 |
| Article 10.2(a) | Vulnerability and patch management | identify and update relevant and trustworthy information resources to build and maintain awareness about vulnerabilities; | Functional | Intersects With | Vulnerability & Patch Management Program (VPMP) | VPM-02 | Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities. | 3 | | VPM-01 |

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

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

Focal Document: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 10.2(b) | Vulnerability and patch management | ensure the performance of automated vulnerability scanning and assessments on ICT assets, with the frequency and scope of these activities commensurate to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of the ICT asset. For the ICT assets supporting critical or important functions it shall be performed at least on a weekly basis; | Functional | Intersects With | Vulnerability Scanning | VPM-12 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | | VPM-06 |
| Article 10.2(c) | Vulnerability and patch management | verify that ICT third-party service providers handle vulnerabilities related to the ICT services provided to the financial entity and that they report to the financial entity in a timely manner at least the critical vulnerabilities and statistics and trends. In particular, financial entities shall request that ICT third-party service providers investigate the relevant vulnerabilities, determine the root causes and implement appropriate mitigating actions; | Functional | Intersects With | Review of Third-Party Services | TPM-15 | Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls. | 5 | | TPM-08 |
| Article 10.2(c) | Vulnerability and patch management | verify that ICT third-party service providers handle vulnerabilities related to the ICT services provided to the financial entity and that they report to the financial entity in a timely manner at least the critical vulnerabilities and statistics and trends. In particular, financial entities shall request that ICT third-party service providers investigate the relevant vulnerabilities, determine the root causes and implement appropriate mitigating actions; | Functional | Intersects With | Vulnerability & Patch Management Program (VPMP) | VPM-02 | Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities. | 3 | | VPM-01 |
| Article 10.2(d) | Vulnerability and patch management | track the usage of third-party libraries, including open source, used by ICT services supporting critical or important function, of ICT services developed by the financial entity itself or specifically customised or developed for the financial entity by an ICT third-party service provider. The financial entity, in collaboration with the ICT third-party service provider as appropriate, shall monitor the version and possible updates of the third-party libraries. In case of ready to use (off-the-shelf) ICT assets or components of ICT assets acquired and used in the operation of ICT services not supporting critical or important functions, the financial entity shall track to the extent possible the usage of third-party libraries, including open-source ones; | Functional | Intersects With | Third-Party Libraries | CFG-17.1 | Mechanisms exist to restrict the use and import of third-party libraries and/or software components to trustworthy sources. | 3 | | CFG-09.1 |
| Article 10.2(d) | Vulnerability and patch management | track the usage of third-party libraries, including open source, used by ICT services supporting critical or important function, of ICT services developed by the financial entity itself or specifically customised or developed for the financial entity by an ICT third-party service provider. The financial entity, in collaboration with the ICT third-party service provider as appropriate, shall monitor the version and possible updates of the third-party libraries. In case of ready to use (off-the-shelf) ICT assets or components of ICT assets acquired and used in the operation of ICT services not supporting critical or important functions, the financial entity shall track to the extent possible the usage of third-party libraries, including open-source ones; | Functional | Intersects With | Software Bill of Materials (SBOM) | TDA-21.4 | Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses. | 5 | | TDA-04.2 |
| Article 10.2(e) | Vulnerability and patch management | establish procedures for responsible disclosure of vulnerabilities to clients and counterparts as well as to the public, as appropriate; | Functional | Intersects With | Disclosure of Vulnerabilities | TDA-07 | Mechanisms exist to disclose information about vulnerabilities to relevant stakeholders, including:<br>(1) A description of the vulnerability(ies);<br>(2) Affected product(s) and/or service(s);<br>(3) Potential impact of the vulnerability(ies);<br>(4) Severity of the vulnerability(ies); and<br>(5) Guidance to remediate the vulnerability(ies). | 5 | | TDA-02.11 |
| Article 10.2(e) | Vulnerability and patch management | establish procedures for responsible disclosure of vulnerabilities to clients and counterparts as well as to the public, as appropriate; | Functional | Intersects With | Vulnerability Disclosure Program (VDP) | THR-12 | Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Technology Assets, Applications and/or Services (TAAS) that receives unsolicited input from the public about vulnerabilities in organizational TAAS. | 3 | | THR-06 |
| Article 10.2(f) | Vulnerability and patch management | identify criteria to prioritise the deployment of patches and other mitigation measures to address the vulnerabilities identified. For the purposes of the prioritisation, financial entities shall consider the criticality of the vulnerability, the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and the risk profile of the ICT assets affected by the identified vulnerabilities; | Functional | Intersects With | Vulnerability Ranking | VPM-05 | Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information. | 5 | | VPM-03 |
| Article 10.2(f) | Vulnerability and patch management | identify criteria to prioritise the deployment of patches and other mitigation measures to address the vulnerabilities identified. For the purposes of the prioritisation, financial entities shall consider the criticality of the vulnerability, the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and the risk profile of the ICT assets affected by the identified vulnerabilities; | Functional | Intersects With | Vulnerability Remediation Process | VPM-06 | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. | 3 | | VPM-02 |
| Article 10.2(g) | Vulnerability and patch management | monitor and verify the remediation of vulnerabilities; | Functional | Intersects With | Vulnerability Remediation Process | VPM-06 | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. | 5 | | VPM-02 |
| Article 10.2(h) | Vulnerability and patch management | require the recording of any detected vulnerabilities affecting ICT systems and the monitoring of their resolution. | Functional | Intersects With | Vulnerability Remediation Process | VPM-06 | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. | 5 | | VPM-02 |
| Article 10.3 | Vulnerability and patch management | As part of the ICT security procedures, financial entities shall develop, document and implement patch management procedures with a view to ensuring the security of networks and enabling safeguards against intrusions and data misuse in order to preserve the availability, authenticity, integrity and confidentiality of data. | 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. | 8 | | OPS-01.1 |
| Article 10.3 | Vulnerability and patch management | As part of the ICT security procedures, financial entities shall develop, document and implement patch management procedures with a view to ensuring the security of networks and enabling safeguards against intrusions and data misuse in order to preserve the availability, authenticity, integrity and confidentiality of data. | Functional | Intersects With | Vulnerability & Patch Management Policy | VPM-01 | Mechanisms exist to establish a formal, documented vulnerability and patch management policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors; | 5 | | |
| Article 10.3 | Vulnerability and patch management | As part of the ICT security procedures, financial entities shall develop, document and implement patch management procedures with a view to ensuring the security of networks and enabling safeguards against intrusions and data misuse in order to preserve the availability, authenticity, integrity and confidentiality of data. | Functional | Intersects With | Vulnerability & Patch Management Program (VPMP) | VPM-02 | Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities. | 3 | | VPM-01 |
| Article 10.3 | Vulnerability and patch management | As part of the ICT security procedures, financial entities shall develop, document and implement patch management procedures with a view to ensuring the security of networks and enabling safeguards against intrusions and data misuse in order to preserve the availability, authenticity, integrity and confidentiality of data. | Functional | Intersects With | Software & Firmware Patching | VPM-08 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 8 | | VPM-05 |
| Article 10.4 | Vulnerability and patch management | The patch management procedures referred to in paragraph 3 shall: | 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 |
| Article 10.4(a) | Vulnerability and patch management | identify and evaluate available software and hardware patches and updates using automated tools, to the extent possible; | 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 |
| Article 10.4(a) | Vulnerability and patch management | identify and evaluate available software and hardware patches and updates using automated tools, to the extent possible; | Functional | Intersects With | Automated Software & Firmware Updates | VPM-08.1 | Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates. | 3 | | VPM-05.4 |
| Article 10.4(b) | Vulnerability and patch management | identify emergency procedures for the patching and updating of ICT assets; | Functional | Intersects With | Out-of-Cycle Patching | VPM-11 | Mechanisms exist to perform out-of-cycle software and/or firmware updates to address time-sensitive remediations. | 8 | | VPM-05.7 |
| Article 10.4(c) | Vulnerability and patch management | test and deploy software and hardware patches and updates in accordance with Article 8(2), point (b), points (v), (vi) and (vii); | Functional | Intersects With | Separation of Development, Testing and Operational Environments | TDA-15.1 | Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production Technology Assets, Applications and/or Services (TAAS). | 3 | | TDA-08 |
| Article 10.4(c) | Vulnerability and patch management | test and deploy software and hardware patches and updates in accordance with Article 8(2), point (b), points (v), (vi) and (vii); | Functional | Intersects With | Pre-Deployment Patch Testing | VPM-10 | Mechanisms exist to perform due diligence on software and/or firmware update stability by conducting pre-production testing in a non-production environment. | 8 | | VPM-05.6 |
| Article 10.4(d) | Vulnerability and patch management | set deadlines for the installation of software and hardware patches and updates and escalation procedures in case the deadline cannot be met. | Functional | Intersects With | Time To Remediate / Benchmarks For Corrective Action | VPM-07 | Mechanisms exist to track the effectiveness of remediation operations through metrics reporting. | 8 | | VPM-05.3 |

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

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

**Focal Document:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 11.1 | Data and system security | As part of the ICT security procedures, with a view to ensuring the security of networks and information systems against intrusions and data misuse, in order to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement a data and ICT system security procedure. | Functional | Intersects With | Data Protection | DCH-02 | Mechanisms exist to facilitate the implementation of data protection controls. | 5 | | DCH-01 |
| Article 11.1 | Data and system security | As part of the ICT security procedures, with a view to ensuring the security of networks and information systems against intrusions and data misuse, in order to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement a data and ICT system security procedure. | 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. | 8 | | OPS-01.1 |
| Article 11.2 | Data and system security | The data and ICT system security procedure referred to in paragraph 1 shall include all of the following elements related to data and ICT system security, in accordance with the classification performed pursuant to Article 8(1) of Regulation (EU) 2022/2554: | Functional | Intersects With | Data Protection | DCH-02 | Mechanisms exist to facilitate the implementation of data protection controls. | 5 | | DCH-01 |
| Article 11.2 | Data and system security | The data and ICT system security procedure referred to in paragraph 1 shall include all of the following elements related to data and ICT system security, in accordance with the classification performed pursuant to Article 8(1) of Regulation (EU) 2022/2554: | Functional | Intersects With | Data & Asset Classification | DCH-04 | Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements. | 3 | | DCH-02 |
| Article 11.2(a) | Data and system security | the access restrictions, in line with Article 21, supporting the protection requirements for each level of classification; | Functional | Intersects With | Defining Access Authorizations for Sensitive / Regulated Data | DCH-06.1 | Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and/or physical access to sensitive and/or regulated data. | 5 | | DCH-01.4 |
| Article 11.2(a) | Data and system security | the access restrictions, in line with Article 21, supporting the protection requirements for each level of classification; | 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 |
| Article 11.2(b) | Data and system security | identification of secure configuration baseline for ICT assets that will minimise their exposure to cyber threats and measures to verify regularly that these baselines are those that are effectively deployed. The secure configuration baseline shall take into account leading practices and appropriate techniques referred to in standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012; | Functional | Intersects With | Secure Baseline Configurations | CFG-04 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards. | 8 | | CFG-02 |
| Article 11.2(b) | Data and system security | identification of secure configuration baseline for ICT assets that will minimise their exposure to cyber threats and measures to verify regularly that these baselines are those that are effectively deployed. The secure configuration baseline shall take into account leading practices and appropriate techniques referred to in standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012; | Functional | Intersects With | Automated Baseline Configuration Management & Verification | CFG-07.1 | Automated mechanisms exist to govern and report on secure baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies. | 5 | | CFG-02.2 |
| Article 11.2(c) | Data and system security | identification of security measures to ensure that only authorised software is installed in ICT systems and endpoint devices; | Functional | Intersects With | Restrict Roles Permitted To Install Software | CFG-12 | Automated mechanisms exist to prevent the installation of software, unless the action is performed by a privileged user or service. | 5 | | CFG-05 |
| Article 11.2(c) | Data and system security | identification of security measures to ensure that only authorised software is installed in ICT systems and endpoint devices; | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-14.1 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 5 | | CFG-03.3 |
| Article 11.2(d) | Data and system security | identification of security measures against malicious codes; | Functional | Intersects With | Malicious Code Protection (Antimalware) | END-04 | Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code. | 8 | | END-04 |
| Article 11.2(e) | Data and system security | identification of security measures to ensure that only authorised data storage media, ICT systems and endpoint devices are used to transfer and store data of the financial entity; | Functional | Intersects With | Digital Media Use Restrictions | DCH-19 | Mechanisms exist to restrict the use of types of digital media on systems or system components. | 5 | | DCH-10 |
| Article 11.2(e) | Data and system security | identification of security measures to ensure that only authorised data storage media, ICT systems and endpoint devices are used to transfer and store data of the financial entity; | Functional | Intersects With | Removable Media Security | DCH-21 | Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters. | 3 | | DCH-12 |
| Article 11.2(f) | Data and system security | requirements to secure the use of portable endpoint devices and private non-portable endpoint devices as follows: | Functional | Intersects With | Endpoint Protection Mechanisms | END-03 | Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices. | 5 | | END-02 |
| Article 11.2(f) | Data and system security | requirements to secure the use of portable endpoint devices and private non-portable endpoint devices as follows: | Functional | Intersects With | Centralized Management Of | MDM-02 | Mechanisms exist to implement and govern Mobile Device Management (MDM) controls. | 5 | | MDM-01 |
| Article 11.2(f)(i) | Data and system security | the use of a management solution to remotely manage the endpoint devices and remotely wipe the financial entity's data; | Functional | Intersects With | Centralized Management Of Mobile Devices | MDM-02 | Mechanisms exist to implement and govern Mobile Device Management (MDM) controls. | 5 | | MDM-01 |
| Article 11.2(f)(i) | Data and system security | the use of a management solution to remotely manage the endpoint devices and remotely wipe the financial entity's data; | Functional | Intersects With | Remote Purging | MDM-09 | Mechanisms exist to remotely purge selected information from mobile devices. | 8 | | MDM-05 |
| Article 11.2(f)(ii) | Data and system security | the use of security mechanisms that cannot be modified, removed or bypassed by staff members or ICT third-party service providers in an unauthorised manner; | Functional | Intersects With | Integrity Assurance & Enforcement (IAE) | CFG-08.2 | Automated mechanisms exist to:<br>(1) Identify unauthorized deviations from an approved secure baseline configuration; and<br>(2) Implement automated resiliency actions to remediate the unauthorized change. | 3 | | CFG-06 |
| Article 11.2(f)(ii) | Data and system security | the use of security mechanisms that cannot be modified, removed or bypassed by staff members or ICT third-party service providers in an unauthorised manner; | Functional | Intersects With | Restrict Access To Security Functions | CFG-21 | Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions. | 5 | | END-16 |
| Article 11.2(f)(iii) | Data and system security | the authorisation to use removable data storage devices only where the residual ICT risk remains within the financial entity's risk tolerance level referred to in Article 3, paragraph 1, point (a); | Functional | Intersects With | Portable Storage Devices | DCH-20 | Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems. | 5 | | DCH-13.2 |
| Article 11.2(f)(iii) | Data and system security | the authorisation to use removable data storage devices only where the residual ICT risk remains within the financial entity's risk tolerance level referred to in Article 3, paragraph 1, point (a); | Functional | Intersects With | Removable Media Security | DCH-21 | Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters. | 5 | | DCH-12 |
| Article 11.2(g) | Data and system security | the process to securely delete data, present on premises or stored externally, that the financial entity no longer needs to collect or to store; | Functional | Intersects With | Digital & Non-Digital Media Disposal | DCH-17 | Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures. | 8 | | DCH-21 |
| Article 11.2(h) | Data and system security | the process to securely dispose or decommission of data storage devices present on premises or stored externally containing confidential information; | Functional | Intersects With | Digital & Non-Digital Media Disposal | DCH-17 | Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures. | 5 | | DCH-08 |
| Article 11.2(h) | Data and system security | the process to securely dispose or decommission of data storage devices present on premises or stored externally containing confidential information; | Functional | Intersects With | Digital Media Sanitization | DCH-18 | Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse. | 5 | | DCH-09 |
| Article 11.2(i) | Data and system security | the identification and implementation of security measures to prevent data loss and leakage for ICT systems and endpoint devices; | 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 | 8 | | NET-17 |
| Article 11.2(j) | Data and system security | the implementation of security measures to ensure that teleworking and the use of private endpoint devices does not adversely impact the ICT security of the financial entity; | Functional | Intersects With | Use of Personal Devices | AST-25 | Mechanisms exist to restrict the possession and/or use of personally-owned Technology Assets, Applications and/or Services (TAAS) within organization-controlled facilities. | 5 | | AST-12 |
| Article 11.2(j) | Data and system security | the implementation of security measures to ensure that teleworking and the use of private endpoint devices does not adversely impact the ICT security of the financial entity; | Functional | Intersects With | Work From Anywhere (WFA) - Telecommuting Security | NET-27 | Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers. | 8 | | NET-14.5 |
| Article 11.2(k) | Data and system security | for ICT assets or services operated by an ICT third-party service provider, the identification and implementation of requirements to maintain digital operational resilience, in accordance with the results of the data classification and ICT risk assessment. In identifying these requirements, financial entities shall consider at least the following: | Functional | Intersects With | Defined Operational Resilience Requirements | BCD-02.1 | Mechanisms exist to define operational resilience requirements for Technology Assets, Applications, Services and/or Data (TAASD) to operate in a controlled and acceptable manner during:<br>(1) Routine operations; and | 5 | | |
| Article 11.2(k) | Data and system security | for ICT assets or services operated by an ICT third-party service provider, the identification and implementation of requirements to maintain digital operational resilience, in accordance with the results of the data classification and ICT risk assessment. In identifying these requirements, financial entities shall consider at least the following: | 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 |
| Article 11.2(k) | Data and system security | for ICT assets or services operated by an ICT third-party service provider, the identification and implementation of requirements to maintain digital operational resilience, in accordance with the results of the data classification and ICT risk assessment. In identifying these requirements, financial entities shall consider at least the following: | Functional | Intersects With | Third-Party Contract Requirements | TPM-14 | Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or | 3 | | TPM-05 |

**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:** **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 11.2(k)(i) | Data and system security | implementation of vendor recommended settings on the elements operated by the financial entity; | Functional | Intersects With | Secure Baseline Configurations | CFG-04 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards. | 5 | | CFG-02 |
| Article 11.2(k)(ii) | Data and system security | clear allocation of information security roles and responsibilities between the financial entity and the ICT third-party service provider, in accordance with the principle of full responsibility of the financial entity referred to in Article 28(1), point (a), of Regulation (EU) 2022/2554, and, for financial entities referred to in Article 28(2) of the same Regulation, with [Article 3] of Commission Delegated Regulation (EU) XXXX/XXX [Commission Delegated Regulation supplementing Article 28(2) of Regulation (EU) 2022/2554; | Functional | Intersects With | Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix | TPM-11 | Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs). | 8 | | TPM-05.4 |
| Article 11.2(k)(iii) | Data and system security | ensuring and maintaining adequate competences within the financial entity in the management and security of the service used; | 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. | 5 | | HRS-03.2 |
| Article 11.2(k)(iii) | Data and system security | ensuring and maintaining adequate competences within the financial entity in the management and security of the service used; | 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 | 5 | | HRS-13 |
| Article 11.2(k)(iv) | Data and system security | technical and organisational measures to minimise the risks related to the infrastructure used by the ICT third-party service provider for its ICT services, considering leading practices and standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012. | Functional | Intersects With | Supply Chain Risk Management (SCRM) | TPM-04 | Mechanisms exist to:<br>(1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and<br>(2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary. | 3 | | TPM-03 |
| Article 11.2(k)(iv) | Data and system security | technical and organisational measures to minimise the risks related to the infrastructure used by the ICT third-party service provider for its ICT services, considering leading practices and standards, as defined in Article 2, point (1), of Regulation (EU) No 1025/2012. | 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 |
| Article 12.1 | Logging | As part of the safeguards against intrusions and data misuse and to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement logging procedures, protocols and tools. | Functional | Intersects With | Continuous Monitoring | MON-02 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 5 | | MON-01 |
| Article 12.2 | Logging | The logging procedures, protocols and tools shall include all of the following: | Functional | Intersects With | Continuous Monitoring | MON-02 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 5 | | MON-01 |
| Article 12.2(a) | Logging | the identification of the events to be logged, the retention period of the logs and the measures to secure and handle the log data, considering the purpose for which the logs are created. The retention period shall be defined taking into account the business and information security objectives, the reason for recording the event in the logs and the results of the ICT risk assessment; | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5 | | MON-03 |
| Article 12.2(a) | Logging | the identification of the events to be logged, the retention period of the logs and the measures to secure and handle the log data, considering the purpose for which the logs are created. The retention period shall be defined taking into account the business and information security objectives, the reason for recording the event in the logs and the results of the ICT risk assessment; | Functional | Intersects With | Protection of Event Logs & Security-Relevant Telemetry | MON-12 | Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion. | 3 | | MON-08 |
| Article 12.2(a) | Logging | the identification of the events to be logged, the retention period of the logs and the measures to secure and handle the log data, considering the purpose for which the logs are created. The retention period shall be defined taking into account the business and information security objectives, the reason for recording the event in the logs and the results of the ICT risk assessment; | 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 |
| Article 12.2(b) | Logging | alignment of the level of detail of the logs with their purpose and usage to enable the effective detection of anomalous activities as specified in Article 24; | Functional | Intersects With | Audit Level Adjustments | MON-03.3 | Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence. | 3 | | MON-02.6 |
| Article 12.2(b) | Logging | alignment of the level of detail of the logs with their purpose and usage to enable the effective detection of anomalous activities as specified in Article 24; | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5 | | MON-03 |
| Article 12.2(c) | Logging | the requirement to log events related to all of the following: | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5 | | MON-03 |
| Article 12.2(c)(i) | Logging | identity management in accordance with Article 20 and logical and physical access control, in accordance with Article 21 and; | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5 | | MON-03 |
| Article 12.2(c)(i) | Logging | identity management in accordance with Article 20 and logical and physical access control, in accordance with Article 21 and; | Functional | Intersects With | Monitoring Physical Access | PES-13 | Physical access control mechanisms exist to monitor for, detect and respond to physical security | 3 | | PES-05 |
| Article 12.2(c)(ii) | Logging | capacity management; | Functional | Intersects With | Performance Monitoring | CAP-05 | Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical Technology Assets, Applications and/or Services (TAAS). | 3 | | CAP-04 |
| Article 12.2(c)(ii) | Logging | capacity management; | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 3 | | MON-03 |
| Article 12.2(c)(iii) | Logging | change management; | 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 | 3 | | CHG-02.2 |

**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:** **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 12.2(c)(iii) | Logging | change management; | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 3 | | MON-03 |
| Article 12.2(c)(iv) | Logging | ICT operations, including ICT system activities; | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5 | | MON-03 |
| Article 12.2(c)(v) | Logging | network traffic activities, including ICT network performance; | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5 | | MON-03 |
| Article 12.2(c)(v) | Logging | network traffic activities, including ICT network performance; | Functional | Intersects With | Inbound & Outbound Communications Traffic | MON-22 | Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions. | 5 | | MON-01.3 |
| Article 12.2(d) | Logging | measures to protect logging systems and log information against tampering, deletion and unauthorised access at rest, in transit and, where relevant, in use; | 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. | 8 | | MON-08 |
| Article 12.2(e) | Logging | measures to detect failure of logging systems; | Functional | Intersects With | Response To Event Log Processing Failures | MON-33 | Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption. | 8 | | MON-05 |
| Article 12.2(e) | Logging | measures to detect failure of logging systems; | Functional | Intersects With | Real-Time Alerts of Event Logging Failure | MON-33.1 | Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs. | 5 | | MON-05.1 |
| Article 12.2(f) | Logging | without prejudice to any applicable regulatory requirements under national or Union law, the synchronisation of the clocks of each of the financial entity's ICT systems upon a documented reliable reference time source. | Functional | Intersects With | Synchronization With Authoritative Time Source | MON-11.1 | Mechanisms exist to synchronize internal system clocks with an authoritative time source. | 8 | | MON-07.1 |
| Article 12.2(f) | Logging | without prejudice to any applicable regulatory requirements under national or Union law, the synchronisation of the clocks of each of the financial entity's ICT systems upon a documented reliable reference time source. | Functional | Intersects With | Clock Synchronization | SEA-30 | Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks. | 5 | | SEA-20 |
| Title II - Chapter I - Section VI | Network Security | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 13.1 | Network security management | As part of the safeguards to ensuring the security of networks against intrusions and data misuse and in order to preserve the availability, authenticity, integrity and confidentiality of data financial entities shall develop, document and implement policies, procedures, protocols and tools on network security management, including all of the following elements: | Functional | Intersects With | Network Security Controls (NSC) | NET-02 | Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC). | 8 | | NET-01 |
| Article 13.1(a) | Network security management | the segregation and segmentation of ICT systems and networks taking into account the criticality or importance of the function they support, the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of ICT assets using them; | Functional | Intersects With | Network Segmentation (macrosegmentation) | NET-06 | Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources. | 8 | | NET-06 |
| Article 13.1(a) | Network security management | the segregation and segmentation of ICT systems and networks taking into account the criticality or importance of the function they support, the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and the overall risk profile of ICT assets using them; | Functional | Intersects With | Isolation of System Components | NET-42.1 | Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions. | 5 | | NET-03.7 |
| Article 13.1(b) | Network security management | the documentation of all of the financial entity's network connections and data flows; | Functional | Intersects With | Network Diagrams & Data Flow Diagrams (DFDs) | AST-17 | Mechanisms exist to maintain network architecture diagrams that:<br>(1) Contain sufficient detail to assess the security of the network's architecture;<br>(2) Reflect the current architecture of the network environment; and<br>(3) Document all sensitive and/or regulated data flows. | 8 | | AST-04 |
| Article 13.1(c) | Network security management | the use of a separate and dedicated network for the administration of ICT assets; | Functional | Intersects With | Security Management Subnets | NET-06.1 | Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system. | 8 | | NET-06.1 |
| Article 13.1(d) | Network security management | the identification and implementation of network access controls to prevent and detect connections to the financial entity's network by any unauthorised device or system, or any endpoint not meeting the financial entity's security requirements; | Functional | Intersects With | Identification & Authentication for Devices | IAC-34 | Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant. | 3 | | IAC-04 |
| Article 13.1(d) | Network security management | the identification and implementation of network access controls to prevent and detect connections to the financial entity's network by any unauthorised device or system, or any endpoint not meeting the financial entity's security requirements; | Functional | Intersects With | Network Access Control (NAC) | NET-16 | Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices. | 8 | | AST-02.5 |
| Article 13.1(d) | Network security management | the identification and implementation of network access controls to prevent and detect connections to the financial entity's network by any unauthorised device or system, or any endpoint not meeting the financial entity's security requirements; | 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 |
| Article 13.1(e) | Network security management | the encryption of network connections passing over corporate networks, public networks, domestic networks, third-party networks and wireless networks, for communication protocols used taking into account the results of the approved data classification and the results of the ICT risk assessment and in accordance with Article 6(2); | Functional | Intersects With | Wireless Access Authentication & Encryption | CFG-04.8 | Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption. | 3 | | CRY-07 |
| Article 13.1(e) | Network security management | the encryption of network connections passing over corporate networks, public networks, domestic networks, third-party networks and wireless networks, for communication protocols used taking into account the results of the approved data classification and the results of the ICT risk assessment and in accordance with Article 6(2); | Functional | Intersects With | Encrypting Data In Transit | CRY-05 | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit. | 5 | | CRY-03 |
| Article 13.1(e) | Network security management | the encryption of network connections passing over corporate networks, public networks, domestic networks, third-party networks and wireless networks, for communication protocols used taking into account the results of the approved data classification and the results of the ICT risk assessment and in accordance with Article 6(2); | Functional | Intersects With | Safeguarding Data Over Open Networks | NET-37 | Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive and/or regulated data during transmission over open, public networks. | 5 | | NET-12 |
| Article 13.1(f) | Network security management | the design of networks in accordance with ICT security requirements and taking into account leading practices to ensure the confidentiality, integrity and availability of the network; | Functional | Intersects With | Secure Engineering Principles | SEA-05 | Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS). | 5 | | SEA-01 |

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

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

**Focal Document:** **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 13.1(f) | Network security management | the design of networks in accordance with ICT security requirements and taking into account leading practices to ensure the confidentiality, integrity and availability of the network; | Functional | Intersects With | Defense-In-Depth (DiD) Architecture | SEA-06 | Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers. | 5 | | NET-02 |
| Article 13.1(g) | Network security management | the securing of network traffic between the internal networks and the internet and other external connections; | Functional | Intersects With | Boundary Protection | NET-03 | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network. | 8 | | NET-03 |
| Article 13.1(h) | Network security management | the identification of the roles and responsibilities and steps for the definition, implementation, approval, change and review of firewall rules and connections filters. Financial entities shall perform the review of firewall rules and connections filters on a regular basis according to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and overall risk profile of ICT systems involved. For the ICT systems supporting critical or important functions, the financial entities shall verify the adequacy of the existing firewall rules and connection filters at least every six months; | Functional | Intersects With | Data Flow Enforcement – Access Control Lists (ACLs) | NET-04 | Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized. | 5 | | NET-04 |
| Article 13.1(h) | Network security management | the identification of the roles and responsibilities and steps for the definition, implementation, approval, change and review of firewall rules and connections filters. Financial entities shall perform the review of firewall rules and connections filters on a regular basis according to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and overall risk profile of ICT systems involved. For the ICT systems supporting critical or important functions, the financial entities shall verify the adequacy of the existing firewall rules and connection filters at least every six months; | Functional | Intersects With | Human Reviews | NET-04.2 | Mechanisms exist to enforce the use of human reviews for Access Control Lists (ACLs) and similar rulesets on a routine basis. | 8 | | NET-04.6 |
| Article 13.1(i) | Network security management | the performance of reviews of the network architecture and of the network security design once a year, and periodically for microenterprises, to identify potential vulnerabilities; | 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 |
| Article 13.1(i) | Network security management | the performance of reviews of the network architecture and of the network security design once a year, and periodically for microenterprises, to identify potential vulnerabilities; | 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 |
| Article 13.1(j) | Network security management | the measures to temporarily isolate, where necessary, subnetworks and network components and devices; | Functional | Intersects With | Dynamic Isolation & Segregation (Sandboxing) | NET-42.2 | Automated mechanisms exist to dynamically isolate (e.g., sandbox) untrusted components during runtime, where the component is isolated in a fault-contained environment but it can still collaborate with the application. | 5 | | NET-03.6 |
| Article 13.1(j) | Network security management | the measures to temporarily isolate, where necessary, subnetworks and network components and devices; | Functional | Intersects With | Host Containment | NET-43 | Automated mechanisms exist to enforce host containment protections that revoke or quarantine a host's access to the network. | 5 | | NET-08.3 |
| Article 13.1(k) | Network security management | the implementation of a secure configuration baseline of all network components and hardening the network and network devices according to vendor instructions, to, where applicable, standards as defined in Article 2, point (1), of Regulation (EU) No 1025/2012 and leading practices; | 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 |
| Article 13.1(l) | Network security management | the procedures to limit, lock and terminate system and remote sessions after a predefined period of inactivity; | Functional | Intersects With | Session Lock | CFG-04.3 | Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods. | 5 | | IAC-24 |
| Article 13.1(l) | Network security management | the procedures to limit, lock and terminate system and remote sessions after a predefined period of inactivity; | Functional | Intersects With | Session Termination | CFG-04.5 | Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity. | 5 | | IAC-25 |
| Article 13.1(l) | Network security management | the procedures to limit, lock and terminate system and remote sessions after a predefined period of inactivity; | Functional | Intersects With | Network Connection Termination | NET-28 | Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity. | 5 | | NET-07 |
| Article 13.1(m) | Network security management | with reference to network services agreements, the identification and definition of ICT and information security measures, service levels and management requirements of all network services, whether these services are provided by an ICT intra-group service provider or by ICT third-party service providers; | Functional | Intersects With | Interconnection Security Agreements (ISAs) | NET-05 | Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection:<br>(1) Interface characteristics;<br>(2) Security, compliance and resilience requirements; and;<br>(3) The nature of the information communicated. | 5 | | NET-05 |
| Article 13.1(m) | Network security management | with reference to network services agreements, the identification and definition of ICT and information security measures, service levels and management requirements of all network services, whether these services are provided by an ICT intra-group service provider or by ICT third-party service providers; | Functional | Intersects With | Third-Party Contract Requirements | TPM-14 | Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or | 5 | | TPM-05 |
| Article 14.1 | Securing information in transit | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement the policies, procedures, protocols and tools to protect information in transit. In particular, financial entities shall ensure all of the following: | Functional | Intersects With | Encrypting Data In Transit | CRY-05 | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit. | 5 | | CRY-03 |
| Article 14.1 | Securing information in transit | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement the policies, procedures, protocols and tools to protect information in transit. In particular, financial entities shall ensure all of the following: | Functional | Intersects With | Integrity of Data In Transit | CRY-06 | Cryptographic mechanisms exist to detect unauthorized changes to data in transit. | 5 | | CRY-04 |
| Article 14.1 | Securing information in transit | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement the policies, procedures, protocols and tools to protect information in transit. In particular, financial entities shall ensure all of the following: | Functional | Intersects With | Safeguarding Data Over Open Networks | NET-37 | Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive and/or regulated data during transmission over open, public networks. | 3 | | NET-12 |
| Article 14.1(a) | Securing information in transit | the availability, authenticity, integrity and confidentiality of data during network transmission, as well as the establishment of procedures to assess compliance with these requirements; | Functional | Intersects With | Encrypting Data In Transit | CRY-05 | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit. | 5 | | CRY-03 |
| Article 14.1(a) | Securing information in transit | the availability, authenticity, integrity and confidentiality of data during network transmission, as well as the establishment of procedures to assess compliance with these requirements; | Functional | Intersects With | Integrity of Data In Transit | CRY-06 | Cryptographic mechanisms exist to detect unauthorized changes to data in transit. | 5 | | CRY-04 |
| Article 14.1(b) | Securing information in transit | the prevention and detection of data leakage and the secure transfer of information between the financial entity and external parties; | Functional | Intersects With | Sensitive / Regulated Data Sharing Decisions | DCH-08.1 | Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected. | 5 | | DCH-14 |
| Article 14.1(b) | Securing information in transit | the prevention and detection of data leakage and the secure transfer of information between the financial entity and external parties; | 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 | 8 | | NET-17 |
| Article 14.1(c) | Securing information in transit | that requirements on confidentiality or non-disclosure arrangements reflecting the financial entity's needs for the protection of information for both the staff of the financial entity and of third parties are implemented, documented and regularly reviewed. | Functional | Intersects With | Confidentiality Agreements | HRS-07.1 | Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, for both employees and third-parties. | 8 | | HRS-06.1 |
| Article 14.2 | Securing information in transit | The policies, procedures, protocols and tools to protect information in transit referred to in paragraph 1 shall take into account the results of the approved data classification and the ICT risk assessment | Functional | Intersects With | Data & Asset Classification | DCH-04 | Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements. | 3 | | DCH-02 |

**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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 14.2 | Securing information in transit | The policies, procedures, protocols and tools to protect information in transit referred to in paragraph 1 shall take into account the results of the approved data classification and the ICT risk assessment processes. | 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 |
| Title II - Chapter I - Section VII | ICT Project and Change Management | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 15.1 | ICT project management | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement an ICT project management policy. | Functional | Subset Of | Project & Resource Management Policy | PRM-01 | Mechanisms exist to establish a formal, documented project and resource management policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors;<br>(3) Is reviewed at least annually; and<br>(4) Is updated, as necessary, to adapt to evolving | 10 | | |
| Article 15.1 | ICT project management | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement an ICT project management policy. | 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 |
| Article 15.2 | ICT project management | The ICT project management policy shall define the elements to ensure the effective management of the ICT projects related to the acquisition, maintenance and, where applicable, development of the financial entity's ICT systems. | 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 |
| Article 15.2 | ICT project management | The ICT project management policy shall define the elements to ensure the effective management of the ICT projects related to the acquisition, maintenance and, where applicable, development of the financial entity's ICT systems. | 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 |
| Article 15.2 | ICT project management | The ICT project management policy shall define the elements to ensure the effective management of the ICT projects related to the acquisition, maintenance and, where applicable, development of the financial entity's ICT systems. | Functional | Intersects With | Project & Resource Management Policy | PRM-01 | Mechanisms exist to establish a formal, documented project and resource management policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors;<br>(3) Is reviewed at least annually; and<br>(4) Is updated, as necessary, to adapt to evolving | 5 | | |
| Article 15.3 | ICT project management | The ICT project management policy shall include all of the following elements: | Functional | Intersects With | Project & Resource Management Policy | PRM-01 | Mechanisms exist to establish a formal, documented project and resource management policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors;<br>(3) Is reviewed at least annually; and<br>(4) Is updated, as necessary, to adapt to evolving | 5 | | |
| Article 15.3 | ICT project management | The ICT project management policy shall include all of the following elements: | 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 |
| Article 15.3(a) | ICT project management | 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 |
| Article 15.3(b) | ICT project management | project governance, including roles and responsibilities; | Functional | Intersects With | Defined Roles & Responsibilities | HRS-04 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 3 | | HRS-03 |
| Article 15.3(b) | ICT project management | project governance, including 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 |
| Article 15.3(c) | ICT project management | project planning, 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 |
| Article 15.3(d) | ICT project management | 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 |
| Article 15.3(d) | ICT project management | 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 |
| Article 15.3(e) | ICT project management | relevant 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 |
| Article 15.3(e) | ICT project management | relevant milestones; | Functional | Intersects With | Project Management Stage Gates | PRM-08.1 | Mechanisms exist to embed formal checkpoints placed between project management stages to ensure security, compliance and resilience controls are integrated early into the development lifecycle. | 5 | | |
| Article 15.3(f) | ICT project management | 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 |
| Article 15.3(f) | ICT project management | 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 |
| Article 15.3(g) | ICT project management | testing of all requirements, including security requirements, and the respective approval process when deploying an ICT system in 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 |

**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:** **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 15.3(g) | ICT project management | testing of all requirements, including security requirements, and the respective approval process when deploying an ICT system in 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:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and | 5 | | TDA-09 |
| Article 15.4 | ICT project management | The ICT project management policy shall ensure the secure ICT project implementation through the provision of the necessary information and expertise from the business area or functions impacted by the ICT project. | 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 |
| Article 15.4 | ICT project management | The ICT project management policy shall ensure the secure ICT project implementation through the provision of the necessary information and expertise from the business area or functions impacted by the ICT project. | 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 |
| Article 15.5 | ICT project management | The ICT project management policy shall provide that the establishment and progress of ICT projects impacting critical or important functions and their associated risks shall be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, periodically and, where necessary, on an event-driven basis, in accordance with ICT project risk assessment included in paragraph 3, point (d). | 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 |
| Article 15.5 | ICT project management | The ICT project management policy shall provide that the establishment and progress of ICT projects impacting critical or important functions and their associated risks shall be reported to the management body, individually or in aggregation, depending on the importance and size of the ICT projects, periodically and, where necessary, on an event-driven basis, in accordance with ICT project risk assessment included in paragraph 3, point (d). | 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 |
| Article 16.1 | ICT systems acquisition, development, and maintenance | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement a policy governing the acquisition, development and maintenance of ICT systems. This policy shall: | 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 | 5 | | PRM-07 |
| Article 16.1 | ICT systems acquisition, development, and maintenance | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement a policy governing the acquisition, development and maintenance of ICT systems. This policy shall: | Functional | Subset Of | Technology Development & Acquisition Policy | TDA-01 | Mechanisms exist to establish a formal, documented technology development and acquisition policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected | 10 | | |
| Article 16.1 | ICT systems acquisition, development, and maintenance | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement a policy governing the acquisition, development and maintenance of ICT systems. This policy shall: | 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 |
| Article 16.1(a) | ICT systems acquisition, development, and maintenance | identify security practices and methodologies relating to the acquisition, development and maintenance of ICT systems; | 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. | 5 | | TDA-01 |
| Article 16.1(a) | ICT systems acquisition, development, and maintenance | identify security practices and methodologies relating to the acquisition, development and maintenance of ICT systems; | Functional | Intersects With | Secure Software Development Practices (SSDP) | TDA-05 | Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP). | 5 | | TDA-06 |
| Article 16.1(b) | ICT systems acquisition, development, and maintenance | require the identification of technical specification and ICT technical specification, as respectively defined in Article 2, points (4) and (5), of Regulation (EU) No 1025/2012, of requirements relating to acquisition, development and maintenance of ICT systems, with a particular focus on ICT security requirements and on their approval by the relevant business function and ICT asset owner according to the financial entity's internal governance arrangements; | Functional | Intersects With | Security, Compliance & Resilience Requirements Definition | PRM-09 | Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by:<br>(1) Defining technical security, compliance and resilience requirements; and<br>(2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC). | 8 | | PRM-05 |
| Article 16.1(b) | ICT systems acquisition, development, and maintenance | require the identification of technical specification and ICT technical specification, as respectively defined in Article 2, points (4) and (5), of Regulation (EU) No 1025/2012, of requirements relating to acquisition, development and maintenance of ICT systems, with a particular focus on ICT security requirements and on their approval by the relevant business function and ICT asset owner according to the financial entity's internal governance arrangements; | 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 |
| Article 16.1(c) | ICT systems acquisition, development, and maintenance | define measures to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development, maintenance and deployment 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 |
| Article 16.1(c) | ICT systems acquisition, development, and maintenance | define measures to mitigate the risk of unintentional alteration or intentional manipulation of the ICT systems during development, maintenance and deployment 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 |
| Article 16.2 | ICT systems acquisition, development, and maintenance | Financial entities shall develop, document and implement an ICT systems' acquisition, development and maintenance procedure, which shall include all of the following: | 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. | 5 | | TDA-01 |
| Article 16.2(a) | ICT systems acquisition, development, and maintenance | the requirements to test and approve all ICT systems prior to their use and after maintenance, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). The level of testing shall be commensurate to the criticality of the concerned business functions and ICT assets. The testing shall be designed to verify that new ICT systems are adequate to perform as intended, including the quality of the software developed internally. | 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 |
| Article 16.2(a) | ICT systems acquisition, development, and maintenance | the requirements to test and approve all ICT systems prior to their use and after maintenance, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). The level of testing shall be commensurate to the criticality of the concerned business functions and ICT assets. The testing shall be designed to verify that new ICT systems are adequate to perform as intended, including the quality of the software developed internally. | 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:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and | 5 | | TDA-09 |
| Article 16.2(b) | ICT systems acquisition, development, and maintenance | the requirements to perform source code reviews covering both static and dynamic testing. The testing shall include security testing for internet-exposed systems and applications, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). Financial entities shall identify and analyse vulnerabilities and anomalies in the source code, adopt an action plan to address them and monitor their implementation. | Functional | Intersects With | Static Code Analysis | TDA-17.1 | Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis. | 5 | | TDA-09.2 |
| Article 16.2(b) | ICT systems acquisition, development, and maintenance | the requirements to perform source code reviews covering both static and dynamic testing. The testing shall include security testing for internet-exposed systems and applications, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). Financial entities shall identify and analyse vulnerabilities and anomalies in the source code, adopt an action plan to address them and monitor their implementation. | Functional | Intersects With | Dynamic Code Analysis | TDA-17.2 | Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis. | 5 | | TDA-09.3 |
| Article 16.2(b) | ICT systems acquisition, development, and maintenance | the requirements to perform source code reviews covering both static and dynamic testing. The testing shall include security testing for internet-exposed systems and applications, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). Financial entities shall identify and analyse vulnerabilities and anomalies in the source code, adopt an action plan to address them and monitor their implementation. | Functional | Intersects With | Developer Threat Analysis & Flaw Remediation | TDA-20.1 | Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production. | 3 | | TDA-15 |

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

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

**Focal Document:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 16.2(c) | ICT systems acquisition, development, and maintenance | the requirements to perform security testing of software packages at no later than the integration phase, in accordance with Article 8(2), point (b), points (v), (vi) and (vii). | 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:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and | 5 | | TDA-09 |
| Article 16.2(d) | ICT systems acquisition, development, and maintenance | the requirement that non-production environments only store anonymized, pseudonymized or randomized production data and that financial entities shall protect the integrity and confidentiality of data in non-production environments. | 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. | 5 | | DCH-18.2 |
| Article 16.2(d) | ICT systems acquisition, development, and maintenance | the requirement that non-production environments only store anonymized, pseudonymized or randomized production data and that financial entities shall protect the integrity and confidentiality of data in non-production environments. | Functional | Intersects With | Use of Live Data | TDA-18 | Mechanisms exist to approve, document and control the use of live data in development and test environments. | 8 | | TDA-10 |
| Article 16.2(e) | ICT systems acquisition, development, and maintenance | the requirement to implement controls to protect the integrity of the source code of ICT systems that are developed in-house or by an ICT third-party service provider and delivered to the financial entity by an ICT third-parties service provider; | 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 |
| Article 16.2(e) | ICT systems acquisition, development, and maintenance | the requirement to implement controls to protect the integrity of the source code of ICT systems that are developed in-house or by an ICT third-party service provider and delivered to the financial entity by an ICT third-parties service provider; | Functional | Intersects With | Software / Firmware Integrity Verification | TDA-20.3 | Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components. | 3 | | TDA-14.1 |
| Article 16.2(f) | ICT systems acquisition, development, and maintenance | the requirement that proprietary software and, where feasible, the source code provided by ICT third-party service providers or coming from open-source projects, shall be analysed and tested prior to their deployment in the production environment. | Functional | Intersects With | Open Source Software | CFG-13 | Mechanisms exist to establish parameters for the secure use of open source software. | 5 | | CFG-04.1 |
| Article 16.2(f) | ICT systems acquisition, development, and maintenance | the requirement that proprietary software and, where feasible, the source code provided by ICT third-party service providers or coming from open-source projects, shall be analysed and tested prior to their deployment in 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:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and | 5 | | TDA-09 |
| Article 16.3 | ICT systems acquisition, development, and maintenance | For the purposes of the testing according to paragraph 2, point (a): | 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:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and | 3 | | TDA-09 |
| Article 16.3(a) | ICT systems acquisition, development, and maintenance | central counterparties shall involve, as appropriate, in the design and conduct of these tests, clearing members and clients, interoperable central counterparties and other interested parties; | 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:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and | 3 | | TDA-09 |
| Article 16.3(b) | ICT systems acquisition, development, and maintenance | central securities depositories shall, as appropriate, involve in the design and conduct of these tests: users, critical utilities and critical service providers, other central securities depositories, other market infrastructures and any other institutions with which interdependencies have been identified in its business continuity policy. | 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:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and | 3 | | TDA-09 |
| Article 16.4 | ICT systems acquisition, development, and maintenance | By way of derogation from paragraph 2, point (d), production data that are not anonymized, not pseudonymized or not randomized may be stored only for specific testing occasions, for limited periods of time and following the approval by the relevant function and, for financial entities other than microenterprises, the reporting of such occasions to the ICT risk management function. | 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 |
| Article 16.4 | ICT systems acquisition, development, and maintenance | By way of derogation from paragraph 2, point (d), production data that are not anonymized, not pseudonymized or not randomized may be stored only for specific testing occasions, for limited periods of time and following the approval by the relevant function and, for financial entities other than microenterprises, the reporting of such occasions to the ICT risk management function. | Functional | Intersects With | Use of Live Data | TDA-18 | Mechanisms exist to approve, document and control the use of live data in development and test environments. | 8 | | TDA-10 |
| Article 16.5 | ICT systems acquisition, development, and maintenance | The procedures referred in this Article shall also apply to ICT systems developed or managed by users outside the ICT function, using a risk-based approach. | 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. | 5 | | OPS-07 |
| Article 16.5 | ICT systems acquisition, development, and maintenance | The procedures referred in this Article shall also apply to ICT systems developed or managed by users outside the ICT function, 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. | 3 | | TDA-01 |
| Article 17.1 | ICT change management | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall develop, document and implement ICT change management procedures. | Functional | Subset Of | Change Management Program | CHG-02 | Mechanisms exist to facilitate the implementation of a change management program. | 10 | | CHG-01 |
| Article 17.2 | ICT change management | Financial entities shall include in the ICT change management procedures, in respect of all changes to software, hardware, firmware components, systems or security parameters, all of the following elements: | Functional | Intersects With | Change Management Program | CHG-02 | Mechanisms exist to facilitate the implementation of a change management program. | 5 | | CHG-01 |
| Article 17.2 | ICT change management | Financial entities shall include in the ICT change management procedures, in respect of all changes to software, hardware, firmware components, systems or security parameters, all of the following elements: | Functional | Intersects With | Configuration Change Control | CHG-03 | Mechanisms exist to govern the technical configuration change control processes. | 5 | | CHG-02 |
| Article 17.2(a) | ICT change management | verification that ICT security requirements have been met; | 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. | 8 | | CHG-06 |
| Article 17.2(b) | ICT change management | mechanisms to ensure independence between the functions that approve changes and those responsible for requesting and implementing them; | Functional | Intersects With | Dual Authorization for Changes To Critical / Sensitive Technology Assets, Applications and/or Services (TAAS) | CHG-04.3 | Mechanisms exist to enforce a two-person rule for implementing changes to critical and/or sensitive Technology Assets, Applications and/or Services (TAAS). | 3 | | CHG-04.3 |
| Article 17.2(b) | ICT change management | mechanisms to ensure independence between the functions that approve changes and those responsible for requesting and implementing them; | 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 |
| Article 17.2(c) | ICT change management | definition of clear roles and responsibilities to ensure that changes are defined, planned, that an adequate transition is designed, that the changes are tested and finalised in a controlled manner and that there is an effective quality assurance; | Functional | Intersects With | Change Management Program | CHG-02 | Mechanisms exist to facilitate the implementation of a change management program. | 5 | | CHG-01 |
| Article 17.2(c) | ICT change management | definition of clear roles and responsibilities to ensure that changes are defined, planned, that an adequate transition is designed, that the changes are tested and finalised in a controlled manner and that there is an effective quality assurance; | Functional | Intersects With | Test, Validate & Document Changes | CHG-07 | Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented into production. | 5 | | CHG-02.2 |

**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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 17.2(c) | ICT change management | definition of clear roles and responsibilities to ensure that changes are defined, planned, that an adequate transition is designed, that the changes are tested and finalised in a controlled manner and that there is an effective quality assurance; | Functional | Intersects With | Defined Roles & Responsibilities | HRS-04 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 3 | | HRS-03 |
| Article 17.2(d) | ICT change management | documentation and communication of change details, including purpose and scope of the change, the timeline for implementation and the expected outcomes; | 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 | 3 | | CHG-02.2 |
| Article 17.2(d) | ICT change management | documentation and communication of change details, including purpose and scope of the change, the timeline for implementation and the expected outcomes; | Functional | Intersects With | Stakeholder Notification of Changes | CHG-08 | Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes. | 8 | | CHG-05 |
| Article 17.2(e) | ICT change management | identification of fall-back procedures and responsibilities, including procedures and responsibilities for aborting changes or recovering from changes not successfully implemented; | Functional | Intersects With | Retention Of Previous Configurations | CFG-09 | Mechanisms exist to retain previous versions of secure baseline configuration to support roll back. | 5 | | CFG-02.3 |
| Article 17.2(e) | ICT change management | identification of fall-back procedures and responsibilities, including procedures and responsibilities for aborting changes or recovering from changes not successfully implemented; | Functional | Intersects With | Configuration Change Control | CHG-03 | Mechanisms exist to govern the technical configuration change control processes. | 3 | | CHG-02 |
| Article 17.2(f) | ICT change management | procedures, protocols and tools to manage emergency changes that provide adequate safeguards; | Functional | Intersects With | Emergency Changes | CHG-10 | Mechanisms exist to govern change management procedures for "emergency" changes. | 8 | | CHG-07 |
| Article 17.2(g) | ICT change management | procedures to document, re-evaluate, assess and approve after their implementation emergency changes, including workarounds and patches; | Functional | Intersects With | Documenting Emergency Changes | CHG-10.1 | Mechanisms exist to document the results of "emergency" changes, including an explanation for why standard change management procedures could not be followed. | 8 | | CHG-07.1 |
| Article 17.2(h) | ICT change management | identification of the potential impact of a change on existing ICT security measures and assessment of whether it requires the adoption of additional ICT security measures. | 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 |
| Article 17.3 | ICT change management | After making significant changes to its systems, central counterparties and central securities depositories shall submit their ICT systems to stringent testing by simulating stressed conditions: | Functional | Intersects With | Test, Validate & Document Changes | CHG-07 | Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented into | 5 | | CHG-02.2 |
| Article 17.3(a) | ICT change management | a central counterparty shall involve, as appropriate, in the design and conduct of these tests: clearing members and clients, interoperable central counterparties and other interested parties; | 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 | 3 | | CHG-02.2 |
| Article 17.3(b) | ICT change management | a central securities depositories shall, as appropriate, involve in the design and conduct of these tests: users, critical utilities and critical service providers, other central securities depositories, other market infrastructures and any other institutions with which interdependencies have been identified in its ICT business continuity policy. | 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 |
| Title II - Chapter I - Section VIII | N/A | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 18.1 | Physical and environmental security | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall define, document and implement a physical and environmental security policy, which shall be designed according to the cyber threat landscape, to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and to the overall risk profile of ICT assets and information assets that can be accessed. | Functional | Intersects With | Physical & Environmental Security Policy | PES-01 | Mechanisms exist to establish a formal, documented physical and environmental security policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors;<br>(3) Is reviewed at least annually; and<br>(4) Is updated, as necessary, to adapt to evolving | 8 | | |
| Article 18.1 | Physical and environmental security | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall define, document and implement a physical and environmental security policy, which shall be designed according to the cyber threat landscape, to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and to the overall risk profile of ICT assets and information assets that can be accessed. | Functional | Subset Of | Physical & Environmental Protections | PES-02 | Mechanisms exist to facilitate the operation of physical and environmental protection controls. | 10 | | PES-01 |
| Article 18.1 | Physical and environmental security | As part of the safeguards to preserve the availability, authenticity, integrity and confidentiality of data, financial entities shall define, document and implement a physical and environmental security policy, which shall be designed according to the cyber threat landscape, to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and to the overall risk profile of ICT assets and information assets that can be accessed. | Functional | Intersects With | Physical Security Plan (PSP) | PES-03 | Mechanisms exist to document a Physical Security Plan (PSP), or similar document, to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats. | 5 | | PES-01.1 |
| Article 18.2 | Physical and environmental security | The physical and environmental security policy shall include all of the following: | Functional | Intersects With | Physical & Environmental Security Policy | PES-01 | Mechanisms exist to establish a formal, documented physical and environmental security policy that:<br>(1) Conveys executive management's intent; | 5 | | |
| Article 18.2 | Physical and environmental security | The physical and environmental security policy shall include all of the following: | Functional | Intersects With | Physical & Environmental Protections | PES-02 | Mechanisms exist to facilitate the operation of physical and environmental protection controls. | 5 | | PES-01 |
| Article 18.2(a) | Physical and environmental security | a reference to the section of the policy on control of access management rights referred to in Article 21(1) point (g); | Functional | Intersects With | Physical & Environmental Security Policy | PES-01 | Mechanisms exist to establish a formal, documented physical and environmental security policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors; | 5 | | |
| Article 18.2(a) | Physical and environmental security | a reference to the section of the policy on control of access management rights referred to in Article 21(1) point (g); | Functional | Intersects With | Physical Access Authorizations | PES-06 | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible). | 3 | | PES-02 |
| Article 18.2(b) | Physical and environmental security | measures to protect the premises, data centres of the financial entity and sensitive designated areas identified by the financial entity where ICT assets and information assets reside from attacks, accidents and from environmental threats and hazards. The measures to protect from environmental threats and hazards shall be commensurate with the importance of the premises, data centres, sensitive designated areas and the criticality of the operations or ICT systems located there; | Functional | Intersects With | Physical & Environmental Protections | PES-02 | Mechanisms exist to facilitate the operation of physical and environmental protection controls. | 5 | | PES-01 |
| Article 18.2(b) | Physical and environmental security | measures to protect the premises, data centres of the financial entity and sensitive designated areas identified by the financial entity where ICT assets and information assets reside from attacks, accidents and from environmental threats and hazards. The measures to protect from environmental threats and hazards shall be commensurate with the importance of the premises, data centres, sensitive designated areas and the criticality of the operations or ICT systems located there; | Functional | Intersects With | Physical Security of Offices, Rooms & Facilities | PES-10 | Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities. | 5 | | PES-04 |
| Article 18.2(c) | Physical and environmental security | measures to secure ICT assets, both within and outside the premises of the financial entity, taking into account the results of the ICT risk assessment related to the relevant ICT assets. The physical and environmental security policy shall include measures to provide appropriate protection to unattended ICT assets; | Functional | Intersects With | Unattended End-User Equipment | AST-20 | Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and unauthorized access. | 5 | | AST-06 |
| Article 18.2(c) | Physical and environmental security | measures to secure ICT assets, both within and outside the premises of the financial entity, taking into account the results of the ICT risk assessment related to the relevant ICT assets. The physical and environmental security policy shall include measures to provide appropriate protection to unattended ICT assets; | Functional | Intersects With | Physical & Environmental Security Policy | PES-01 | Mechanisms exist to establish a formal, documented physical and environmental security policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors; | 5 | | |
| Article 18.2(c) | Physical and environmental security | measures to secure ICT assets, both within and outside the premises of the financial entity, taking into account the results of the ICT risk assessment related to the relevant ICT assets. The physical and environmental security policy shall include measures to provide appropriate protection to unattended ICT assets; | Functional | Intersects With | Equipment Siting & Protection | PES-16 | Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. | 5 | | PES-12 |
| Article 18.2(d) | Physical and environmental security | measures to ensure the availability, authenticity, integrity and confidentiality of data information assets and physical access control devices of the financial entity through the appropriate maintenance; | Functional | Intersects With | Controlled Maintenance | MNT-03 | Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS). | 5 | | MNT-02 |
| Article 18.2(e) | Physical and environmental security | measures to preserve the availability, authenticity, integrity and confidentiality of the data, including a clear desk policy for papers and a clear screen policy for information processing facilities. | Functional | Intersects With | Unattended End-User Equipment | AST-20 | Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and | 3 | | AST-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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 18.2(e) | Physical and environmental security | measures to preserve the availability, authenticity, integrity and confidentiality of the data, including a clear desk policy for papers and a clear screen policy for information processing facilities. | Functional | Intersects With | Session Lock | CFG-04.3 | Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods. | 3 | | IAC-24 |
| Title II - Chapter II | Human Resources Policy and Access Control | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 19.1 | Human resources policy | As part of their human resource or other relevant policies financial entities shall include all of the following ICT security related elements: | Functional | Intersects With | Human Resources Security Policy | HRS-01 | Mechanisms exist to establish a formal, documented human resources security policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors;<br>(3) Is reviewed at least annually; and<br>(4) Is updated, as necessary, to adapt to evolving | 5 | | |
| Article 19.1 | Human resources policy | As part of their human resource or other relevant policies financial entities shall include all of the following ICT security related elements: | Functional | Intersects With | Human Resources Security Policy | HRS-01 | Mechanisms exist to establish a formal, documented human resources security policy that: | 5 | | |
| Article 19.1 | Human resources policy | As part of their human resource or other relevant policies financial entities shall include all of the following ICT security related elements: | Functional | Intersects With | Human Resources Security Management | HRS-02 | Mechanisms exist to facilitate the implementation of personnel security controls. | 5 | | HRS-01 |
| Article 19.1(a) | Human resources policy | identification and assignment of any specific ICT security responsibilities; | 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 |
| Article 19.1(a) | Human resources policy | identification and assignment of any specific ICT security responsibilities; | Functional | Intersects With | Defined Roles & Responsibilities | HRS-04 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 8 | | HRS-03 |
| Article 19.1(b) | Human resources policy | requirements for staff of the financial entity and of the ICT third-party service providers using or accessing ICT assets of the financial entity to: | Functional | Intersects With | Terms of Employment | HRS-06 | Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities. | 5 | | HRS-05 |
| Article 19.1(b) | Human resources policy | requirements for staff of the financial entity and of the ICT third-party service providers using or accessing ICT assets of the financial entity to: | Functional | Intersects With | Third-Party Personnel | HRS-13 | Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities. | 3 | | HRS-10 |
| Article 19.1(b)(i) | Human resources policy | be informed about, and adhere to, the financial entity's ICT security policies, procedures and protocols; | Functional | Intersects With | Policy Familiarization & Acknowledgement | HRS-08.2 | Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement. | 8 | | HRS-05.7 |
| Article 19.1(b)(i) | Human resources policy | be informed about, and adhere to, the financial entity's ICT security policies, procedures and protocols; | Functional | Intersects With | Security, Compliance & Resilience Awareness Training | SAT-04 | Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function. | 3 | | SAT-02 |
| Article 19.1(b)(ii) | Human resources policy | be aware of the reporting channels put in place by the financial entity for the purpose of detection of anomalous behaviour, including, where applicable, those established according to Directive (EU) 2019/1937 of the European Parliament and of the Council; | Functional | Intersects With | Reporting Suspicious Activities | HRS-18 | Mechanisms exist to enable personnel to report suspicious activities and/or behavior without fear of reprisal or other negative consequences (e.g., whistleblower protections). | 5 | | HRS-15 |
| Article 19.1(b)(iii) | Human resources policy | upon termination of employment, requirements for the staff to return to the financial entity all ICT assets and tangible information assets in their possession that belong to the financial entity. | Functional | Intersects With | Asset Collection | HRS-12.2 | Mechanisms exist to retrieve organization-owned assets upon termination of an individual's employment. | 8 | | HRS-09.1 |
| Article 20.1 | Identity management | As part of their control of access management rights, financial entities shall develop, document and implement identity management policies and procedures to ensure the unique identification and authentication of natural persons and systems accessing the financial entities' information to enable assignment of user access rights, in accordance with Article 21. | 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 |
| Article 20.1 | Identity management | As part of their control of access management rights, financial entities shall develop, document and implement identity management policies and procedures to ensure the unique identification and authentication of natural persons and systems accessing the financial entities' information to enable assignment of user access rights, in accordance with Article 21. | Functional | Intersects With | Standardized Identifier Management (User Names) | IAC-13.1 | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS). | 3 | | IAC-09 |
| Article 20.1 | Identity management | As part of their control of access management rights, financial entities shall develop, document and implement identity management policies and procedures to ensure the unique identification and authentication of natural persons and systems accessing the financial entities' information to enable assignment of user access rights, in accordance with Article 21. | 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 |
| Article 20.2 | Identity management | These policies and procedures shall include all of the following elements: | 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 |
| Article 20.2(a) | Identity management | without prejudice to Article 21(1), point (c), the assignment of a unique identity corresponding to a unique user account to each staff member of the financial entity or staff of the third-party service providers accessing the information assets and ICT assets of the financial entity; | Functional | Intersects With | Standardized Identifier Management (User Names) | IAC-13.1 | Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS). | 5 | | IAC-09 |
| Article 20.2(a) | Identity management | without prejudice to Article 21(1), point (c), the assignment of a unique identity corresponding to a unique user account to each staff member of the financial entity or staff of the third-party service providers accessing the information assets and ICT assets of the financial entity; | Functional | Intersects With | Identification & Authentication for Organizational Users | IAC-32 | Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users. | 8 | | IAC-02 |
| Article 20.2(b) | Identity management | the maintenance of records of all identity assignments referred to in point (a). These records shall be kept following a reorganisation of the financial entity or after the end of the contractual relationship without prejudice to the retention requirements set out in Union and national law; | Functional | Intersects With | Retain Access Records | IAC-03.2 | Mechanisms exist to retain a record of personnel accountability to ensure there is a record of all access granted to an individual (system and application-wise), who provided the authorization, when the authorization was granted and when the access was last reviewed. | 8 | | IAC-01.1 |
| Article 20.2(c) | Identity management | a lifecycle management process for identities and accounts managing the creation, change, review and update, temporary deactivation and termination of all accounts. Where applicable, financial entities shall deploy automated solutions for the lifecycle identity management process. | 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. | 5 | | IAC-07 |
| Article 20.2(c) | Identity management | a lifecycle management process for identities and accounts managing the creation, change, review and update, temporary deactivation and termination of all accounts. Where applicable, financial entities shall deploy automated solutions for the lifecycle identity management process. | Functional | Intersects With | Account Management | IAC-08 | Mechanisms exist to:<br>(1) Define authorized system account types;<br>(2) Define prohibited system account types; and<br>(3) Proactively govern individual, group, system, service, application, guest and temporary accounts. | 8 | | IAC-15 |
| Article 20.2(c) | Identity management | a lifecycle management process for identities and accounts managing the creation, change, review and update, temporary deactivation and termination of all accounts. Where applicable, financial entities shall deploy automated solutions for the lifecycle identity management process. | Functional | Intersects With | Automated System Account Management (Directory Services) | IAC-08.1 | Automated mechanisms exist to support the management of system accounts (e.g., directory services). | 5 | | IAC-15.1 |
| Article 21.1 | Access control | As part of their control of access management rights, financial entities shall develop, document and implement a policy that includes all of the following elements: | 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 |
| Article 21.1(a) | Access control | assignment of access rights to ICT assets based on need-to-know, need-to-use and least privilege principles, including for remote and emergency access; | Functional | Intersects With | Access Enforcement | IAC-25 | Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege." | 5 | | IAC-20 |
| Article 21.1(a) | Access control | assignment of access rights to ICT assets based on need-to-know, need-to-use and least privilege principles, including for remote and emergency access; | Functional | Intersects With | Least Privilege | IAC-30 | Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business | 8 | | IAC-21 |
| Article 21.1(b) | Access control | segregation of duties designed to prevent unjustified access to critical data or to prevent the allocation of combinations of access rights that may be used to circumvent controls; | Functional | Intersects With | Separation of Duties (SoD) | HRS-14 | Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion. | 8 | | HRS-11 |

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

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

Focal Document: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 21.1(b) | Access control | segregation of duties designed to prevent unjustified access to critical data or to prevent the allocation of combinations of access rights that may be used to circumvent controls; | Functional | Intersects With | Incompatible Roles | HRS-15 | Mechanisms exist to avoid incompatible development-specific roles through limiting and reviewing developer privileges to change hardware, software and firmware components within a production/operational environment. | 5 | | HRS-12 |
| Article 21.1(c) | Access control | provision on user accountability, by limiting to the extent possible the use of generic and shared user accounts and ensuring that users are identifiable for the actions performed in the ICT systems at all times; | 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 |
| Article 21.1(c) | Access control | provision on user accountability, by limiting to the extent possible the use of generic and shared user accounts and ensuring that users are identifiable for the actions performed in the ICT systems at all times; | 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 |
| Article 21.1(d) | Access control | provision on restrictions of access to ICT assets, setting out controls and tools to prevent unauthorised access; | Functional | Intersects With | Access Enforcement | IAC-25 | Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege." | 8 | | IAC-20 |
| Article 21.1(e) | Access control | account management procedures to grant, change or revoke access rights for user and generic accounts, including generic administrator accounts. The procedures shall include provision on all the following: | 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. | 5 | | IAC-07 |
| Article 21.1(e) | Access control | account management procedures to grant, change or revoke access rights for user and generic accounts, including generic administrator accounts. The procedures shall include provision on all the following: | Functional | Intersects With | Account Management | IAC-08 | Mechanisms exist to:<br>(1) Define authorized system account types;<br>(2) Define prohibited system account types; and<br>(3) Proactively govern individual, group, system, service, application, guest and temporary accounts. | 5 | | IAC-15 |
| Article 21.1(e)(i) | Access control | assignment of roles and responsibilities for granting, reviewing and revoking access rights. Retention period for logs shall be defined in accordance with Article 12(2), point (a); | Functional | Intersects With | Defined Roles & Responsibilities | HRS-04 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 3 | | HRS-03 |
| Article 21.1(e)(i) | Access control | assignment of roles and responsibilities for granting, reviewing and revoking access rights. Retention period for logs shall be defined in accordance with Article 12(2), point (a); | 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. | 5 | | IAC-07 |
| Article 21.1(e)(i) | Access control | assignment of roles and responsibilities for granting, reviewing and revoking access rights. Retention period for logs shall be defined in accordance with Article 12(2), point (a); | Functional | Intersects With | Event Log & Security-Relevant Telemetry Retention | MON-13 | Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements. | 3 | | MON-10 |
| Article 21.1(e)(ii) | Access control | assignment of privileged, emergency and administrator access on a need-to-use or an ad-hoc basis for all ICT systems. Where possible, for the performance of administrative tasks on ICT systems, dedicated accounts shall be used. Where applicable, financial entities shall deploy automated solutions for the privileged access management; | 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 |
| Article 21.1(e)(ii) | Access control | assignment of privileged, emergency and administrator access on a need-to-use or an ad-hoc basis for all ICT systems. Where possible, for the performance of administrative tasks on ICT systems, dedicated accounts shall be used. Where applicable, financial entities shall deploy automated solutions for the privileged access management; | Functional | Intersects With | Dedicated Privileged Account | IAC-10.3 | Mechanisms exist to assign dedicated privileged user accounts to be used solely for duties requiring privileged access. | 5 | | IAC-16.4 |
| Article 21.1(e)(ii) | Access control | assignment of privileged, emergency and administrator access on a need-to-use or an ad-hoc basis for all ICT systems. Where possible, for the performance of administrative tasks on ICT systems, dedicated accounts shall be used. Where applicable, financial entities shall deploy automated solutions for the privileged access management; | Functional | Intersects With | Emergency Accounts | IAC-11 | Mechanisms exist to establish and control "emergency access only" accounts. | 3 | | IAC-15.9 |
| Article 21.1(e)(iii) | Access control | revoking of access rights without undue delay upon termination of employment or when the access is no longer necessary; | 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. | 8 | | IAC-07.2 |
| Article 21.1(e)(iii) | Access control | revoking of access rights without undue delay upon termination of employment or when the access is no longer necessary; | Functional | Intersects With | Revocation of Access Authorizations | IAC-29 | Mechanisms exist to revoke logical and physical access authorizations. | 5 | | IAC-20.6 |
| Article 21.1(e)(iv) | Access control | update of access rights where changes are necessary and at least once a year for all ICT systems, other than ICT systems supporting critical or important functions and at least every six months for ICT systems supporting critical or important functions; | Functional | Intersects With | Periodic Review of Individual & Service Account Privileges | IAC-12 | Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as | 8 | | IAC-17 |
| Article 21.1(e)(iv) | Access control | update of access rights where changes are necessary and at least once a year for all ICT systems, other than ICT systems supporting critical or important functions and at least every six months for ICT systems supporting critical or important functions; | Functional | Intersects With | System Account Reviews | IAC-12.1 | Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner. | 3 | | IAC-15.7 |
| Article 21.1(f) | Access control | authentication methods including all of the following: | Functional | Intersects With | Authenticator Management | IAC-14 | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed. | 5 | | IAC-10 |
| Article 21.1(f)(i) | Access control | the use of authentication methods commensurate to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and to the overall risk profile of ICT assets and considering leading practices; | Functional | Intersects With | Authenticator Management | IAC-14 | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed. | 8 | | IAC-10 |
| Article 21.1(f)(ii) | Access control | the use of strong authentication methods in accordance with leading practices and techniques for remote access to the financial entity's network, for privileged access, for access to ICT assets supporting critical or important functions or that are publicly accessible; | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-37 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:<br>(1) Remote network access;<br>(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or<br>(3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data. | 8 | | IAC-06 |
| Article 21.1(f)(ii) | Access control | the use of strong authentication methods in accordance with leading practices and techniques for remote access to the financial entity's network, for privileged access, for access to ICT assets supporting critical or important functions or that are publicly accessible; | 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 |
| Article 21.1(g) | Access control | physical access control measures including: | 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 |
| Article 21.1(g)(i) | Access control | identification and logging of natural persons who are authorised to access premises, data centres and sensitive designated areas identified by the financial entity where ICT and information assets reside. This identification and logging shall be commensurate with the importance of the premises, data centres, sensitive designated areas and the criticality of the operations or ICT systems located there; | Functional | Intersects With | Physical Access Authorizations | PES-06 | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible). | 5 | | PES-02 |
| Article 21.1(g)(i) | Access control | identification and logging of natural persons who are authorised to access premises, data centres and sensitive designated areas identified by the financial entity where ICT and information assets reside. This identification and logging shall be commensurate with the importance of the premises, data centres, sensitive designated areas and the criticality of the operations or ICT systems located there; | Functional | Intersects With | Physical Access Logs | PES-09.1 | Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points. | 5 | | PES-03.3 |
| Article 21.1(g)(ii) | Access control | granting of physical access rights to critical ICT assets to authorised persons only according to the need-to-know, least privilege principles and on an ad-hoc basis; | Functional | Intersects With | Role-Based Physical Access | PES-07 | Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual. | 5 | | PES-02.1 |
| Article 21.1(g)(ii) | Access control | granting of physical access rights to critical ICT assets to authorised persons only according to the need-to-know, least privilege principles and on an ad-hoc basis; | Functional | Intersects With | Access To Critical Systems | PES-12 | Physical access control mechanisms exist to enforce physical access to critical systems or sensitive and/or regulated data, in addition to the physical access controls for the facility. | 5 | | PES-03.4 |
| Article 21.1(g)(iii) | Access control | monitoring of physical access to premises, data centres and sensitive designated areas identified by the financial entity where ICT and information assets or both reside. The monitoring should be commensurate to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and the criticality of the area | Functional | Intersects With | Monitoring Physical Access | PES-13 | Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents. | 8 | | PES-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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 21.1(g)(iii) | Access control | monitoring of physical access to premises, data centres and sensitive designated areas identified by the financial entity where ICT and information assets or both reside. The monitoring should be commensurate to the classification established according to Article 8(1) of Regulation (EU) 2022/2554 and the criticality of the area | Functional | Intersects With | Monitoring Physical Access To Critical Systems | PES-13.2 | Facility security mechanisms exist to monitor physical access to critical systems or sensitive and/or regulated data, in addition to the physical access monitoring of the facility. | 5 | | PES-05.2 |
| Article 21.1(g)(iv) | Access control | review of physical access rights to ensure that unnecessary access rights are promptly revoked. | Functional | Intersects With | Revocation of Access Authorizations | IAC-29 | Mechanisms exist to revoke logical and physical access authorizations. | 5 | | IAC-20.6 |
| Article 21.1(g)(iv) | Access control | review of physical access rights to ensure that unnecessary access rights are promptly revoked. | Functional | Intersects With | Physical Access Authorizations | PES-06 | Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible). | 5 | | PES-02 |
| Title II - Chapter III | ICT-Related Incident Detection and Response | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 22.1 | ICT-related incident management policy | As part of the mechanisms to detect anomalous activities, including ICT network performance issues and ICT-related incidents, financial entities shall develop, document and implement an ICT-related incident policy through which they shall: | Functional | Subset Of | 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. | 10 | | IRO-01 |
| Article 22.1 | ICT-related incident management policy | As part of the mechanisms to detect anomalous activities, including ICT network performance issues and ICT-related incidents, financial entities shall develop, document and implement an ICT-related incident policy through which they shall: | 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. | 5 | | IRO-04 |
| Article 22.1(a) | ICT-related incident management policy | document the ICT-related incident management process referred to in Article 17 of Regulation (EU) 2022/2554; | Functional | Intersects With | Incident Response Operations | IRO-02 | Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents. | 3 | | IRO-01 |
| Article 22.1(a) | ICT-related incident management policy | document the ICT-related incident management process referred to in Article 17 of Regulation (EU) 2022/2554; | Functional | Intersects With | Incident Response Plan (IRP) | IRO-08 | Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders. | 8 | | IRO-04 |
| Article 22.1(b) | ICT-related incident management policy | establish a list of relevant contacts with internal functions and external stakeholders that are directly involved in ICT operations' security, including on detection and monitoring cyber threats, detection of anomalous activities and vulnerability management; | Functional | Intersects With | Integrated Security Incident Response Team (ISIRT) | IRO-11 | Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations. | 3 | | IRO-07 |
| Article 22.1(b) | ICT-related incident management policy | establish a list of relevant contacts with internal functions and external stakeholders that are directly involved in ICT operations' security, including on detection and monitoring cyber threats, detection of anomalous activities and vulnerability management; | Functional | Intersects With | Regulatory & Law Enforcement Contacts | IRO-15 | Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies. | 5 | | IRO-14 |
| Article 22.1(c) | ICT-related incident management policy | establish, implement and operate technical, organisational and operational mechanisms to support the ICT-related incident management process, including mechanisms to enable a prompt detection of anomalous activities and behaviours in accordance with Article 23; | Functional | Intersects With | Incident Handling | IRO-06 | Mechanisms exist to cover:<br>(1) Preparation;<br>(2) Automated event detection or manual incident report intake;<br>(3) Analysis;<br>(4) Containment;<br>(5) Eradication; and<br>(6) Recovery. | 5 | | IRO-02 |
| Article 22.1(c) | ICT-related incident management policy | establish, implement and operate technical, organisational and operational mechanisms to support the ICT-related incident management process, including mechanisms to enable a prompt detection of anomalous activities and behaviours in accordance with Article 23; | 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 |
| Article 22.1(d) | ICT-related incident management policy | retain all evidence relating to ICT-related incidents for a period no longer than necessary for the purposes for which the data is collected, commensurate with the criticality of the affected business functions, supporting processes and ICT and information assets, in accordance with [Article [15] of Commission Delegated Regulation (EU) [...]/[...] [Commission Delegated Regulation on classification of ICT-related incidents] and with any applicable retention requirement according to Union law. This evidence shall be retained in a secure manner. | Functional | Intersects With | Chain of Custody & Forensics | IRO-13 | Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices. | 5 | | IRO-08 |
| Article 22.1(d) | ICT-related incident management policy | retain all evidence relating to ICT-related incidents for a period no longer than necessary for the purposes for which the data is collected, commensurate with the criticality of the affected business functions, supporting processes and ICT and information assets, in accordance with [Article [15] of Commission Delegated Regulation (EU) [...]/[...] [Commission Delegated Regulation on classification of ICT-related incidents] and with any applicable retention requirement according to Union law. This evidence shall be retained in a secure manner. | Functional | Intersects With | Event Log & Security-Relevant Telemetry Retention | MON-13 | Mechanisms exist to retain event logs and security-relevant telemetry for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements. | 3 | | MON-10 |
| Article 22.1(e) | ICT-related incident management policy | establish and implement mechanisms to analyse significant or recurring ICT-related incidents and patterns in the number and the occurrence of ICT-related incidents. | Functional | Intersects With | Root Cause Analysis (RCA) & Lessons Learned | IRO-14 | Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents. | 3 | | IRO-13 |
| Article 22.1(e) | ICT-related incident management policy | establish and implement mechanisms to analyse significant or recurring ICT-related incidents and patterns in the number and the occurrence of ICT-related incidents. | Functional | Intersects With | Incident Pattern Analysis | IRO-17.1 | Mechanisms exist to analyze historical incidents in aggregate to identify:<br>(1) Patterns;<br>(2) Trends; and<br>(3) Other common root causes in order to address the vulnerability and risk. | 5 | | IRO-09.4 |
| Article 22.1(e) | ICT-related incident management policy | establish and implement mechanisms to analyse significant or recurring ICT-related incidents and patterns in the number and the occurrence of ICT-related incidents. | Functional | Intersects With | Recurring Incident Analysis | IRO-17.2 | Mechanisms exist to periodically review incident response activities for the existence of recurring incidents. | 5 | | IRO-09.2 |
| Article 23.1 | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | Financial entities shall set clear roles and responsibilities to effectively detect and respond to ICT-related incidents and anomalous activities. | Functional | Intersects With | Defined Roles & Responsibilities | HRS-04 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 3 | | HRS-03 |
| Article 23.1 | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | Financial entities shall set clear roles and responsibilities to effectively detect and respond to ICT-related incidents and anomalous activities. | 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 |
| Article 23.2 | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | To detect anomalous activities, ICT network performance issues and ICT-related incidents in accordance with Article 10(1) of Regulation (EU) 2022/2554, financial entities shall implement detection mechanisms allowing them to: | Functional | Intersects With | Continuous Monitoring | MON-02 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 5 | | MON-01 |
| Article 23.2 | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | To detect anomalous activities, ICT network performance issues and ICT-related incidents in accordance with Article 10(1) of Regulation (EU) 2022/2554, financial entities shall implement detection mechanisms allowing them to: | 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 |
| Article 23.2(a) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | collect, monitor and analyse all of the following: | Functional | Intersects With | Continuous Monitoring | MON-02 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 5 | | MON-01 |
| Article 23.2(a) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | collect, monitor and analyse all of the following: | Functional | Intersects With | Centralized Event Log & Security-Relevant Telemetry Review & Analysis | MON-05.1 | Automated mechanisms exist to centrally collect, review and analyze event logs and security-relevant telemetry from multiple sources. | 3 | | MON-02.2 |
| Article 23.2(a)(i) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | internal and external factors, including at least the logs collected according to Article 12, information from business and ICT functions and any problem reported by users of the financial entity; | Functional | Intersects With | Event Log & Security-Relevant Telemetry Monitoring | MON-03 | Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures. | 5 | | MON-01.8 |

**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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 23.2(a)(i) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | internal and external factors, including at least the logs collected according to Article 12, information from business and ICT functions and any problem reported by users of the financial entity; | Functional | Intersects With | Centralized Collection of Event Logs & Security-Relevant Telemetry | MON-05 | Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant telemetry. | 5 | | MON-02 |
| Article 23.2(a)(ii) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | potential internal and external cyber threats, considering scenarios commonly used by threat actors and scenarios based on threat intelligence activity; | 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 |
| Article 23.2(a)(ii) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | potential internal and external cyber threats, considering scenarios commonly used by threat actors and scenarios based on threat intelligence activity; | Functional | Intersects With | Threat Intelligence Feeds | THR-04 | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 5 | | THR-03 |
| Article 23.2(a)(ii) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | potential internal and external cyber threats, considering scenarios commonly used by threat actors and scenarios based on threat intelligence activity; | 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 |
| Article 23.2(a)(iii) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | ICT-related incident notification from an ICT third-party service provider of the financial entity detected in the ICT systems and networks of the ICT third-party service provider and which may affect the financial entity; | 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 |
| Article 23.2(b) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | identify anomalous activities and behaviour and implement tools generating alerts for anomalous activities and behaviour, at least for ICT assets and information assets supporting critical or important functions. This shall include tools that provide automated alerts based on pre-defined rules to identify anomalies affecting the completeness and the integrity of the data sources or log collection; | Functional | Intersects With | Automated Incident Responder Alerting | MON-05.5 | Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications. | 5 | | MON-01.12 |
| Article 23.2(b) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | identify anomalous activities and behaviour and implement tools generating alerts for anomalous activities and behaviour, at least for ICT assets and information assets supporting critical or important functions. This shall include tools that provide automated alerts based on pre-defined rules to identify anomalies affecting the completeness and the integrity of the data sources or log collection; | 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. | 8 | | MON-16 |
| Article 23.2(b) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | identify anomalous activities and behaviour and implement tools generating alerts for anomalous activities and behaviour, at least for ICT assets and information assets supporting critical or important functions. This shall include tools that provide automated alerts based on pre-defined rules to identify anomalies affecting the completeness and the integrity of the data sources or log collection; | Functional | Intersects With | Response To Event Log Processing Failures | MON-33 | Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption. | 3 | | MON-05 |
| Article 23.2(c) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | prioritise the alerts referred to in point (b) to allow the detected ICT-related incidents to be managed within the expected resolution time, as defined by financial entities, both during and outside working hours; | 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 |
| Article 23.2(c) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | prioritise the alerts referred to in point (b) to allow the detected ICT-related incidents to be managed within the expected resolution time, as defined by financial entities, both during and outside working hours; | Functional | Intersects With | Event Log & Security-Relevant Telemetry Analysis & Triage | MON-05.2 | Mechanisms exist to ensure event log and security-relevant telemetry reviews include analysis and triage practices that integrate with the organization's established incident response processes. | 5 | | MON-17 |
| Article 23.2(d) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | record, analyse and evaluate any relevant information on all anomalous activities and behaviours automatically or manually. | Functional | Intersects With | Centralized Event Log & Security-Relevant Telemetry Review & Analysis | MON-05.1 | Automated mechanisms exist to centrally collect, review and analyze event logs and security-relevant telemetry from multiple sources. | 5 | | MON-02.2 |
| Article 23.2(d) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | record, analyse and evaluate any relevant information on all anomalous activities and behaviours automatically or manually. | 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 |
| Article 23.3 | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | Any recording of the anomalous activities shall be protected against tampering and unauthorised access at rest, in transit and, where relevant, in use. | 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. | 8 | | MON-08 |
| Article 23.4 | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | The financial entity shall log all relevant information for each detected anomalous activity to enable identification of the date and time of occurrence and detection, and the type of the anomalous activity. | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 8 | | MON-03 |
| Article 23.4 | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | The financial entity shall log all relevant information for each detected anomalous activity to enable identification of the date and time of occurrence and detection, and the type of the anomalous activity. | Functional | Intersects With | Time Stamps | MON-11 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs and security-relevant telemetry. | 3 | | MON-07 |
| Article 23.5 | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | Financial entities shall consider all the following criteria to trigger ICT-related incident detection and response processes: | 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. | 5 | | IRO-03 |
| Article 23.5 | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | Financial entities shall consider all the following criteria to trigger ICT-related incident detection and response processes: | Functional | Intersects With | Incident Handling | IRO-06 | Mechanisms exist to cover:<br>(1) Preparation;<br>(2) Automated event detection or manual incident report intake;<br>(3) Analysis;<br>(4) Containment;<br>(5) Eradication; and<br>(6) Recovery. | 3 | | IRO-02 |
| Article 23.5(a) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | indications that malicious activity may have been carried out in an ICT system or network or that such ICT system or network may have been compromised; | 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. | 5 | | IRO-03 |
| Article 23.5(a) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | indications that malicious activity may have been carried out in an ICT system or network or that such ICT system or network may have been compromised; | Functional | Intersects With | Monitoring for Indicators of Compromise (IOC) | MON-17 | Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC). | 5 | | MON-11.3 |
| Article 23.5(b) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | data losses detected, in relation to the availability, authenticity, integrity and confidentiality of data; | Functional | Intersects With | Data Loss Prevention (DLP) | DCH-40 | Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed. | 3 | | NET-17 |

**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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 23.5(b) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | data losses detected, in relation to the availability, authenticity, integrity and confidentiality of data; | 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 |
| Article 23.5(c) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | adverse impact detected on financial entity's transactions and operations; | Functional | Intersects With | Anomalous Behavior | MON-16 | Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities. | 3 | | MON-16 |
| Article 23.5(d) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | ICT systems' and network unavailability. | 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 |
| Article 23.5(d) | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | ICT systems' and network unavailability. | Functional | Intersects With | Continuous Monitoring | MON-02 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 3 | | MON-01 |
| Article 23.6 | Anomalous activities' detection and criteria for ICT-related incidents' detection and response | When evaluating the criteria set out in paragraph 5, financial entities shall consider the criticality of the services affected. | 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 |
| Title II - Chapter IV | ICT Business Continuity | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 24.1 | Components of the ICT business continuity policy | Financial entities shall include in their ICT business continuity policy all of the following: | Functional | Intersects With | Business Continuity & Disaster Recovery Policy | BCD-01 | Mechanisms exist to establish a formal, documented Business Continuity and Disaster Recovery (BC/DR) policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors; | 8 | | |
| Article 24.1 | Components of the ICT business continuity policy | Financial entities shall include in their ICT business continuity policy all of the following: | 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:<br>(1) Routine operations; and<br>(2) Adverse conditions. | 10 | | BCD-01 |
| Article 24.1(a) | Components of the ICT business continuity policy | definition of the objectives, including the interrelation of ICT and overall business continuity, and considering the results of the business impact analysis (BIA) referred to in Article 11(5) of Regulation (EU) 2022/2554; | 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:<br>(1) Routine operations; and<br>(2) Adverse conditions. | 5 | | BCD-01 |
| Article 24.1(a) | Components of the ICT business continuity policy | definition of the objectives, including the interrelation of ICT and overall business continuity, and considering the results of the business impact analysis (BIA) referred to in Article 11(5) of Regulation (EU) 2022/2554; | 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 |
| Article 24.1(b) | Components of the ICT business continuity policy | definition of the scope, including limitations and exclusions, to be covered by the ICT business continuity arrangements, plans, procedures and mechanisms; | Functional | Intersects With | Business Continuity & Disaster Recovery Policy | BCD-01 | Mechanisms exist to establish a formal, documented Business Continuity and Disaster Recovery (BC/DR) policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors; | 5 | | |
| Article 24.1(b) | Components of the ICT business continuity policy | definition of the scope, including limitations and exclusions, to be covered by the ICT business continuity arrangements, plans, procedures and mechanisms; | 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:<br>(1) Routine operations; and<br>(2) Adverse conditions. | 5 | | BCD-01 |
| Article 24.1(c) | Components of the ICT business continuity policy | definition of the timeframe to be covered by the ICT business continuity arrangements, plans, procedures and mechanisms; | Functional | Intersects With | Business Continuity & Disaster Recovery Policy | BCD-01 | Mechanisms exist to establish a formal, documented Business Continuity and Disaster Recovery (BC/DR) policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors; | 5 | | |
| Article 24.1(c) | Components of the ICT business continuity policy | definition of the timeframe to be covered by the ICT business continuity arrangements, plans, procedures and mechanisms; | 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:<br>(1) Routine operations; and<br>(2) Adverse conditions. | 3 | | BCD-01 |
| Article 24.1(d) | Components of the ICT business continuity policy | description of the criteria to activate and deactivate ICT business continuity plans, ICT response and recovery plans and crisis communications plans; | 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). | 8 | | BCD-01.5 |
| Article 24.1(e) | Components of the ICT business continuity policy | provisions on the governance and organisation including roles, responsibilities and escalation procedures to implement the ICT business continuity policy and to ensure that sufficient resources are available; | Functional | Intersects With | Business Continuity & Disaster Recovery Policy | BCD-01 | Mechanisms exist to establish a formal, documented Business Continuity and Disaster Recovery (BC/DR) policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors; | 5 | | |
| Article 24.1(e) | Components of the ICT business continuity policy | provisions on the governance and organisation including roles, responsibilities and escalation procedures to implement the ICT business continuity policy and to ensure that sufficient resources are available; | 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:<br>(1) Routine operations; and<br>(2) Adverse conditions. | 5 | | BCD-01 |
| Article 24.1(f) | Components of the ICT business continuity policy | provisions on the alignment between the ICT business continuity plans and the overall business continuity plans. The alignment shall concern at least all of the following: | 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. | 8 | | BCD-01.1 |
| Article 24.1(f)(i) | Components of the ICT business continuity policy | potential failure scenarios, including those listed in Article 26(2); | 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 |
| Article 24.1(f)(ii) | Components of the ICT business continuity policy | recovery objectives, specifying that the financial entity shall be able to recover the operations of its critical or important functions after disruptions within a recovery time objective and a recovery point objective; | 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 |
| Article 24.1(g) | Components of the ICT business continuity policy | provisions on the development of ICT business continuity plans for severe business disruptions as part of these plans, and the prioritisationof ICT business continuity actions using a risk-based approach; | Functional | Intersects With | Identify Critical Assets | AST-05 | Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions. | 3 | | BCD-02 |

**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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 24.1(g) | Components of the ICT business continuity policy | provisions on the development of ICT business continuity plans for severe business disruptions as part of these plans, and the prioritisationof ICT business continuity actions using a risk-based approach; | 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 |
| Article 24.1(h) | Components of the ICT business continuity policy | provisions on the development, testing and review of ICT response and recovery plans, in accordance with Articles 25 and 26; | 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 |
| Article 24.1(h) | Components of the ICT business continuity policy | provisions on the development, testing and review of ICT response and recovery plans, in accordance with Articles 25 and 26; | 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 |
| Article 24.1(i) | Components of the ICT business continuity policy | provisions on the review of the effectiveness of the implemented ICT business continuity arrangements, plans, procedures and mechanisms, in accordance with Article 26; | Functional | Intersects With | Ongoing Contingency Planning | BCD-07 | Mechanisms exist to update contingency plans due to changes affecting:<br>(1) People (e.g., personnel changes);<br>(2) Processes (e.g., new, altered or decommissioned business practices, including third-party services);<br>(3) Technologies (e.g., new, altered or decommissioned technologies);<br>(4) Data (e.g., changes to data flows and/or data repositories);<br>(5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or<br>(6) Feedback from contingency plan testing | 5 | | BCD-06 |
| Article 24.1(i) | Components of the ICT business continuity policy | provisions on the review of the effectiveness of the implemented ICT business continuity arrangements, plans, procedures and mechanisms, in accordance with Article 26; | 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 |
| Article 24.1(j) | Components of the ICT business continuity policy | provisions to align the ICT business continuity policy to the communication policy referred to in Article 14(2) of Regulation (EU) 2022/2554 and to the communication and crisis communication actions referred to in Article 11(2), point (e), of Regulation (EU) | 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. | 5 | | BCD-01.6 |
| Article 24.2 | Components of the ICT business continuity policy | In addition to the requirements referred to in paragraph 1, central counterparties shall ensure that their ICT business continuity policy: | Functional | Intersects With | Business Continuity & Disaster Recovery Policy | BCD-01 | Mechanisms exist to establish a formal, documented Business Continuity and Disaster Recovery (BC/DR) policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors; | 5 | | |
| Article 24.2 | Components of the ICT business continuity policy | In addition to the requirements referred to in paragraph 1, central counterparties shall ensure that their ICT business continuity policy: | 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:<br>(1) Routine operations; and<br>(2) Adverse conditions. | 5 | | BCD-01 |
| Article 24.2(a) | Components of the ICT business continuity policy | includes a maximum recovery time for their critical functions that is not higher than two hours. End of day procedures and payments shall be completed on the required time and day in all circumstances; | 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 |
| Article 24.2(b) | Components of the ICT business continuity policy | takes into account external links and interdependencies within the financial infrastructures including trading venues cleared by the central counterparty, securities settlement and payment systems and credit institutions used by the central counterparty or a linked central counterparty; | Functional | Intersects With | Coordinate with Related Plans | BCD-07.3 | Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans. | 5 | | BCD-01.1 |
| Article 24.2(b) | Components of the ICT business continuity policy | takes into account external links and interdependencies within the financial infrastructures including trading venues cleared by the central counterparty, securities settlement and payment systems and credit institutions used by the central counterparty or a linked central counterparty; | 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. | 3 | | BCD-01.2 |
| Article 24.2(c) | Components of the ICT business continuity policy | requires that arrangements are in place to: | 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:<br>(1) Routine operations; and<br>(2) Adverse conditions. | 5 | | BCD-01 |
| Article 24.2(c)(i) | Components of the ICT business continuity policy | ensure the continuity of their critical or important functions based on disaster scenarios. These arrangements shall at least address the availability of adequate human resources, the maximum downtime of critical functions and fail over and recovery to a secondary site; | 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 |
| Article 24.2(c)(i) | Components of the ICT business continuity policy | ensure the continuity of their critical or important functions based on disaster scenarios. These arrangements shall at least address the availability of adequate human resources, the maximum downtime of critical functions and fail over and recovery to a secondary site; | Functional | Intersects With | Failover Capability | BCD-22 | Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD). | 3 | | BCD-12.2 |
| Article 24.2(c)(ii) | Components of the ICT business continuity policy | maintain a secondary processing site capable of ensuring continuity of their critical or important functions identical to the primary site. The secondary processing site shall have a geographical risk profile which is distinct from that of the primary site; | Functional | Intersects With | Alternate Processing Site | BCD-13 | Mechanisms exist to establish an alternate processing site that provides processing capability and security measures equivalent to that of the primary site. | 5 | | BCD-09 |
| Article 24.2(c)(ii) | Components of the ICT business continuity policy | maintain a secondary processing site capable of ensuring continuity of their critical or important functions identical to the primary site. The secondary processing site shall have a geographical risk profile which is distinct from that of the primary site; | Functional | Intersects With | Separation from Primary Processing Site | BCD-13.1 | Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats. | 5 | | BCD-09.1 |
| Article 24.2(c)(iii) | Components of the ICT business continuity policy | maintain or have immediate access to a secondary business site to allow staff to ensure continuity of the service if the primary location of business is not available; | Functional | Intersects With | Alternate Processing Site | BCD-13 | Mechanisms exist to establish an alternate processing site that provides processing capability and security measures equivalent to that of the | 5 | | BCD-09 |
| Article 24.2(c)(iii) | Components of the ICT business continuity policy | maintain or have immediate access to a secondary business site to allow staff to ensure continuity of the service if the primary location of business is not available; | Functional | Intersects With | Alternate Processing Site Accessibility | BCD-13.2 | Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing sites that would impact mitigation and recovery activities, in the event of an area-wide disruption or disaster. | 5 | | BCD-09.2 |
| Article 24.2(c)(iv) | Components of the ICT business continuity policy | consider the need for additional processing sites, in particular if the diversity of the risk profiles of the primary and secondary sites does not provide sufficient confidence that the central counterparty's business continuity objectives will be met in all scenarios. | Functional | Intersects With | Separation from Primary Processing Site | BCD-13.1 | Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats. | 5 | | BCD-09.1 |
| Article 24.3 | Components of the ICT business continuity policy | In addition to the requirements referred to in paragraph 1, central securities depositories shall ensure that their ICT business continuity policy: | Functional | Intersects With | Business Continuity & Disaster Recovery Policy | BCD-01 | Mechanisms exist to establish a formal, documented Business Continuity and Disaster Recovery (BC/DR) policy that:<br>(1) Conveys executive management's intent;<br>(2) Provides organizational direction and expected behaviors; | 5 | | |
| Article 24.3 | Components of the ICT business continuity policy | In addition to the requirements referred to in paragraph 1, central securities depositories shall ensure that their ICT business continuity policy: | 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:<br>(1) Routine operations; and<br>(2) Adverse conditions. | 5 | | BCD-01 |
| Article 24.3(a) | Components of the ICT business continuity policy | takes into account any links and interdependencies to at least users, critical utilities and critical service providers, other central securities depositories and other market infrastructures; | Functional | Intersects With | Coordinate with Related Plans | BCD-07.3 | Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans. | 5 | | BCD-01.1 |
| Article 24.3(a) | Components of the ICT business continuity policy | takes into account any links and interdependencies to at least users, critical utilities and critical service providers, other central securities depositories and other market infrastructures; | 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. | 3 | | BCD-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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 24.3(b) | Components of the ICT business continuity policy | requires its ICT business continuity arrangements to ensure that the recovery time objective for their critical or important functions shall not be longer than two hours. | 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 |
| Article 24.4 | Components of the ICT business continuity policy | In addition to the requirements referred to in paragraph 1, trading venues shall ensure that their ICT business continuity arrangements allow trading can be resumed within or close to two hours of a disruptive incident and that the maximum amount of data that may be lost from any ICT service of the trading venue after a disruptive incident is close to zero. | 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 |
| Article 25.1 | Testing of the ICT business continuity plans | Financial entities shall test the ICT business continuity plans taking into account the financial entity's BIA and the ICT risk assessment referred to in Article 3(1), point (b). | 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 |
| Article 25.1 | Testing of the ICT business continuity plans | Financial entities shall test the ICT business continuity plans taking into account the financial entity's BIA and the ICT risk assessment referred to in Article 3(1), point (b). | 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 |
| Article 25.2 | Testing of the ICT business continuity plans | Financial entities shall assess through the testing of their ICT business continuity plans whether they are able to ensure the continuity of the financial entity's critical or important functions. The testing of the ICT business continuity plan shall: | 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 |
| Article 25.2(a) | Testing of the ICT business continuity plans | be performed on the basis of test scenarios that simulate potential disruptions, including an adequate set of severe but plausible scenarios. The scenarios considered for the development of the business continuity plans shall always be included in the testing; | 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 |
| Article 25.2(b) | Testing of the ICT business continuity plans | include the testing of ICT services provided by ICT third-parties service providers, where applicable. In testing the business continuity plans as regards ICT third-parties services, financial entities shall duly consider scenarios linked to insolvency or failures of the ICT-third party service provider or of political risks in the provider's jurisdiction, where | Functional | Intersects With | Coordinated Testing with Related Plans | BCD-10.1 | Mechanisms exist to coordinate contingency plan testing with internal and external parties responsible for related plans. | 5 | | BCD-04.1 |
| Article 25.2(b) | Testing of the ICT business continuity plans | include the testing of ICT services provided by ICT third-parties service providers, where applicable. In testing the business continuity plans as regards ICT third-parties services, financial entities shall duly consider scenarios linked to insolvency or failures of the ICT-third party service provider or of political risks in the provider's jurisdiction, where | 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 |
| Article 25.2(c) | Testing of the ICT business continuity plans | for financial entities referred to in the second subparagraph of Article 11(6) of Regulation (EU) 2022/2554, include scenarios of switchover from primary ICT infrastructure to the redundant capacity, backups and redundant facilities. The testing shall verify whether at least critical or important functions can be operated appropriately, for a sufficient period of time and whether the normal functioning may be restored; | 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 |
| Article 25.2(c) | Testing of the ICT business continuity plans | for financial entities referred to in the second subparagraph of Article 11(6) of Regulation (EU) 2022/2554, include scenarios of switchover from primary ICT infrastructure to the redundant capacity, backups and redundant facilities. The testing shall verify whether at least critical or important functions can be operated appropriately, for a sufficient period of time and whether the normal functioning may be restored; | Functional | Intersects With | Test Restoration Using Sampling | BCD-32.1 | Mechanisms exist to utilize sampling of available data backups to test recovery capabilities as part of business continuity plan testing. | 5 | | BCD-11.5 |
| Article 25.2(d) | Testing of the ICT business continuity plans | be designed to challenge the assumptions on which the business continuity plans rest, including governance arrangements and crisis communication plans; | 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 |
| Article 25.2(e) | Testing of the ICT business continuity plans | include procedures to verify the ability of the staff of financial entities, ICT third- party service providers, ICT systems and ICT services to respond adequately to the scenarios duly taken into account in Article 26(2). | 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 |
| Article 25.2(e) | Testing of the ICT business continuity plans | include procedures to verify the ability of the staff of financial entities, ICT third- party service providers, ICT systems and ICT services to respond adequately to the scenarios duly taken into account in Article 26(2). | 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 |
| Article 25.3 | Testing of the ICT business continuity plans | In addition to the requirements referred to in paragraph 2, for central counterparties the testing of their ICT business continuity plans shall include the involvement of clearing members, external providers and relevant institutions in the financial infrastructure with which interdependencies have been identified in their business continuity policies. | 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 |
| Article 25.4 | Testing of the ICT business continuity plans | In addition to the requirements referred to in paragraph 2, for central securities depositories the testing of their ICT business continuity plans shall include the participation of, as appropriate, users of the central securities depositories, critical utilities and critical service providers, other central securities depositories, other market infrastructures and any other institutions with which interdependencies have been identified in their business continuity policy. | 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 |
| Article 25.5 | Testing of the ICT business continuity plans | Test results shall be documented and any identified deficiencies resulting from the tests shall 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 |
| Article 25.5 | Testing of the ICT business continuity plans | Test results shall be documented and any identified deficiencies resulting from the tests shall 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 |
| Article 26.1 | ICT response and recovery plans | Financial entities shall develop ICT response and recovery plans taking into account the results of the BIA. The ICT response and recovery plans shall: | 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 |
| Article 26.1 | ICT response and recovery plans | Financial entities shall develop ICT response and recovery plans taking into account the results of the BIA. The ICT response and recovery plans shall: | 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 |
| Article 26.1(a) | ICT response and recovery plans | specify the conditions prompting their activation, deactivation and any exceptions; | 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). | 8 | | BCD-01.5 |
| Article 26.1(b) | ICT response and recovery plans | describe what actions shall be taken to ensure the availability, integrity, continuity and recovery of at least ICT systems and services supporting critical or important functions of the financial entities; | 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 |
| Article 26.1(b) | ICT response and recovery plans | describe what actions shall be taken to ensure the availability, integrity, continuity and recovery of at least ICT systems and services supporting critical or important functions of the financial entities; | Functional | Intersects With | Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | BCD-18 | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure. | 5 | | BCD-12 |
| Article 26.1(c) | ICT response and recovery plans | be designed to meet the recovery objectives of the operations of the financial entities; | 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 |
| Article 26.1(d) | ICT response and recovery plans | be documented and made available to the staff involved in their execution and be readily accessible in case of emergency. Financial entities shall clearly define roles and responsibilities to that extent; | 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 |
| Article 26.1(e) | ICT response and recovery plans | provide for both short-term and long-term recovery options including partial systems recovery; | 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 |

**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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 26.1(e) | ICT response and recovery plans | provide for both short-term and long-term recovery options including partial systems recovery; | Functional | Intersects With | Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution | BCD-18 | Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure. | 3 | | BCD-12 |
| Article 26.1(f) | ICT response and recovery plans | lay down the objectives and the conditions to declare a successful execution of the plans. | Functional | Intersects With | Recovery Operations Criteria | BCD-05 | Mechanisms exist to define specific criteria that must be met to initiate Business Continuity / Disaster Recovery (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 3 | | BCD-01.5 |
| Article 26.2 | ICT response and recovery plans | The ICT response and recovery plans shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. The response and recovery plans shall develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. Financial entities shall duly take into account all of the following scenarios: | 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 |
| Article 26.2 | ICT response and recovery plans | The ICT response and recovery plans shall identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. The response and recovery plans shall develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. Financial entities shall duly take into account all of the following scenarios: | Functional | Intersects With | Contingency Plan Root Cause Analysis (RCA) & Lessons Learned | BCD-11 | Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated. | 3 | | BCD-05 |
| Article 26.2(a) | ICT response and recovery plans | cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities; | 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 |
| Article 26.2(a) | ICT response and recovery plans | cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities; | 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 |
| Article 26.2(b) | ICT response and recovery plans | scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly consider the potential impact of the insolvency or other failures of any relevant ICT third-party service provider; | 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 |
| Article 26.2(b) | ICT response and recovery plans | scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly consider the potential impact of the insolvency or other failures of any relevant ICT third-party service provider; | Functional | Intersects With | Third-Party Incident Response & Recovery Capabilities | TPM-21 | Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers. | 3 | | TPM-11 |
| Article 26.2(c) | ICT response and recovery plans | partial or total failure of premises, including office and business premises, and data centres; | 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 |
| Article 26.2(c) | ICT response and recovery plans | partial or total failure of premises, including office and business premises, and data centres; | Functional | Intersects With | Alternate Processing Site | BCD-13 | Mechanisms exist to establish an alternate processing site that provides processing capability and security measures equivalent to that of the | 3 | | BCD-09 |
| Article 26.2(d) | ICT response and recovery plans | substantial failure of ICT assets or of the communication infrastructure; | 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 |
| Article 26.2(d) | ICT response and recovery plans | substantial failure of ICT assets or of the communication infrastructure; | Functional | Intersects With | Telecommunications Services Availability | BCD-17 | Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services. | 3 | | BCD-10 |
| Article 26.2(e) | ICT response and recovery plans | the non-availability of a critical number of staff or staff members in charge of guaranteeing the continuity of 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 |
| Article 26.2(e) | ICT response and recovery plans | the non-availability of a critical number of staff or staff members in charge of guaranteeing the continuity of operations; | Functional | Intersects With | Personnel Transfer to Alternate Processing / Storage Site | BCD-16.1 | Mechanisms exist to redeploy personnel to other roles during a disruptive event or in the execution of a continuity plan. | 3 | | BCD-01.3 |
| Article 26.2(f) | ICT response and recovery plans | impact of climate change and environment degradation related events, natural disasters, pandemic, and physical attacks, including intrusions and terrorist attacks; | 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 |
| Article 26.2(g) | ICT response and recovery plans | insider attacks; | 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 |
| Article 26.2(h) | ICT response and recovery plans | political and social instability, including, where relevant, in the jurisdiction from where the ICT third-party service provider provides its services and the location where the data is stored and processed; | 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 |
| Article 26.2(i) | ICT response and recovery plans | widespread power outages. | 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 |
| Article 26.3 | ICT response and recovery plans | The ICT response and recovery plans shall consider alternative options where the primary recovery measures 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 |
| Article 26.3 | ICT response and recovery plans | The ICT response and recovery plans shall consider alternative options where the primary recovery measures 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 |
| Article 26.4 | ICT response and recovery plans | As part of the ICT response and recovery plans, financial entities shall consider and implement continuity measures to mitigate failures of ICT third-party service providers of ICT services supporting critical or important functions to the financial entity. | 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 |
| Article 26.4 | ICT response and recovery plans | As part of the ICT response and recovery plans, financial entities shall consider and implement continuity measures to mitigate failures of ICT third-party service providers of ICT services supporting critical or important functions to the financial entity. | 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 |
| Title II - Chapter V | Report on the ICT Risk Management Framework Review | 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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 27.1 | Format and content | Financial entities shall develop and document the report referred to in Article 6(5) of Regulation (EU) 2022/2554 in a searchable electronic format. | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.1 | Format and content | Financial entities shall develop and document the report referred to in Article 6(5) of Regulation (EU) 2022/2554 in a searchable electronic format. | 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:<br>(1) The organization's Enterprise Risk Management (ERM); and<br>(2) Industry-recognized cybersecurity risk management practices. | 5 | | RSK-01 |
| Article 27.2 | Format and content | Financial entities shall include all of the following information in the report: | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(a) | Format and content | an introductory section which: | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(a)(i) | Format and content | clearly identifies the financial entity, the subject of the report and describes its group structure, where relevant; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 3 | | GOV-17 |
| Article 27.2(a)(ii) | Format and content | describes the context of the report in terms of the nature, scale and complexity of the financial entity's services, activities and operations, its organisation, identified critical functions, strategy, major ongoing projects or activities, relationships and its dependence on in-house and contracted ICT services and systems or the implications that a total loss or severe degradation of such systems would have in terms of critical or important functions and market efficiency; | Functional | Intersects With | Identify Critical Assets | AST-05 | Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions. | 3 | | BCD-02 |
| Article 27.2(a)(ii) | Format and content | describes the context of the report in terms of the nature, scale and complexity of the financial entity's services, activities and operations, its organisation, identified critical functions, strategy, major ongoing projects or activities, relationships and its dependence on in-house and contracted ICT services and systems or the implications that a total loss or severe degradation of such systems would have in terms of critical or important functions and market efficiency; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(a)(iii) | Format and content | summarises the major changes in the ICT risk management framework since the previous report; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(a)(iv) | Format and content | provides an executive level summary of the current and near-term ICT risk profile, threat landscape, the assessed effectiveness of its controls and the security posture of the financial entity; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(a)(iv) | Format and content | provides an executive level summary of the current and near-term ICT risk profile, threat landscape, the assessed effectiveness of its controls and the security posture of the financial entity; | 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 |
| Article 27.2(b) | Format and content | date of the approval of the report by the management body of the financial entity; | 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 |
| Article 27.2(c) | Format and content | description of the reason for the review of the ICT risk management framework in accordance with Article 6(5) of Regulation (EU) 2022/2554. Where the review was initiated following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes, the report shall contain explicit references to such documents or instructions, allowing for the identification of the reason for initiating the review. Where the review was initiated following ICT-related incidents, the report shall contain the list of all ICT-related incidents with incident root-cause analysis; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(c) | Format and content | description of the reason for the review of the ICT risk management framework in accordance with Article 6(5) of Regulation (EU) 2022/2554. Where the review was initiated following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes, the report shall contain explicit references to such documents or instructions, allowing for the identification of the reason for initiating the review. Where the review was initiated following ICT-related incidents, the report shall contain the list of all ICT-related incidents with incident root-cause analysis; | Functional | Intersects With | Incident Tracking Repository | IRO-17 | Mechanisms exist to maintain a repository of cybersecurity events and incidents that documents:<br>(1) Details of the incident (e.g., category, severity and affected parties);<br>(2) Remediation actions taken through incident closure; and<br>(3) A summary from the Root Cause Analysis (RCA), if applicable. | 3 | | IRO-09.3 |
| Article 27.2(d) | Format and content | start and end dates of the review period; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 3 | | GOV-17 |
| Article 27.2(e) | Format and content | indication of the function responsible for the review; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 3 | | GOV-17 |
| Article 27.2(f) | Format and content | description of the major changes and improvements to the ICT risk management framework since the previous review. This description shall include an analysis of the impact of the changes on the financial entity's digital operational resilience strategy, on the financial entity's ICT internal control framework and on the financial entity's ICT risk management governance; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(g) | Format and content | summary of the findings of the review and detailed analysis and assessment of the severity of the weaknesses, deficiencies and gaps in the ICT risk management framework during the review period; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(g) | Format and content | summary of the findings of the review and detailed analysis and assessment of the severity of the weaknesses, deficiencies and gaps in the ICT risk management framework during the review period; | 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:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 5 | | IAO-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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 27.2(h) | Format and content | description of the measures to address identified weaknesses, deficiencies and gaps, including all of the following: | 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:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 5 | | IAO-05 |
| Article 27.2(h) | Format and content | description of the measures to address identified weaknesses, deficiencies and gaps, including all of the following: | Functional | Intersects With | Risk Remediation | RSK-17 | Mechanisms exist to remediate risks to an acceptable level. | 5 | | RSK-06 |
| Article 27.2(h)(i) | Format and content | summary of measures taken to remediate to identified weaknesses, deficiencies and gaps; | 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:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 5 | | IAO-05 |
| Article 27.2(h)(i) | Format and content | summary of measures taken to remediate to identified weaknesses, deficiencies and gaps; | 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:<br>(1) Assessments;<br>(2) Audits; and/or<br>(3) Incidents. | 3 | | RSK-06.1 |
| Article 27.2(h)(ii) | Format and content | expected date for implementing the measures and dates related to the internal control of the implementation, including information on the state of progress of their implementation as at the date of drafting of the report, explaining, where applicable, if there is a risk that deadlines may not be respected; | 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:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 5 | | IAO-05 |
| Article 27.2(h)(ii) | Format and content | expected date for implementing the measures and dates related to the internal control of the implementation, including information on the state of progress of their implementation as at the date of drafting of the report, explaining, where applicable, if there is a risk that deadlines may not be respected; | Functional | Intersects With | Risk Treatment Plan (RTP) | RSK-17.1 | Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline. | 3 | | RSK-06.4 |
| Article 27.2(h)(iii) | Format and content | tools to be used and identification of the function responsible for carrying out the measures, detailing whether they are internal or external; | 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:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 5 | | IAO-05 |
| Article 27.2(h)(iii) | Format and content | tools to be used and identification of the function responsible for carrying out the measures, detailing whether they are internal or external; | Functional | Intersects With | Risk Owner | RSK-11 | Mechanisms exist to identify a risk owner for each item in the risk register to ensure clear accountability for unremediated risks. | 3 | | RSK-03.2 |
| Article 27.2(h)(iv) | Format and content | description of the impact of the changes envisaged in the measures on the financial entity's budgetary, human and material resources, including resources dedicated to the implementation of corrective measures; | Functional | Intersects With | Capabilities Deficiency Tracking | IAO-12 | Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 5 | | IAO-05 |
| Article 27.2(h)(iv) | Format and content | description of the impact of the changes envisaged in the measures on the financial entity's budgetary, human and material resources, including resources dedicated to the implementation of corrective measures; | Functional | Intersects With | Allocation of Resources | PRM-06 | Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives. | 3 | | PRM-03 |
| Article 27.2(h)(v) | Format and content | information on the process for informing the competent authority, where appropriate; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(h)(v) | Format and content | information on the process for informing the competent authority, where appropriate; | Functional | Intersects With | Contacts With Authorities | GOV-15 | Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies. | 3 | | GOV-06 |

**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:** **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 27.2(h)(vi) | Format and content | if the weaknesses, deficiencies or gaps identified are not subject to remedial measures, a detailed explanation of the criteria used to analyse their impact, to evaluate the related residual risk and for the acceptance of such a risk; | Functional | Intersects With | Risk Tolerance | RSK-05.1 | Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results. | 5 | | RSK-01.3 |
| Article 27.2(h)(vi) | Format and content | if the weaknesses, deficiencies or gaps identified are not subject to remedial measures, a detailed explanation of the criteria used to analyse their impact, to evaluate the related residual risk and for the acceptance of such a risk; | Functional | Intersects With | Risk Treatment Options | RSK-16.1 | Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including:<br>(1) Mitigating the risk to an acceptable level;<br>(2) Avoiding the risk (e.g., terminating the project);<br>(3) Transferring the risk to a third party (e.g., insurance and service provider); or<br>(4) Accepting the risk. | 3 | | RSK-06.3 |
| Article 27.2(i) | Format and content | information on planned further developments; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(j) | Format and content | conclusions resulting from the review of the ICT risk management framework; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(k) | Format and content | information on past reviews: | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(k)(i) | Format and content | list of past reviews to date; | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 3 | | GOV-17 |
| Article 27.2(k)(ii) | Format and content | if applicable, state of implementation of the mitigation measures identified by the last report; | 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:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 5 | | IAO-05 |
| Article 27.2(k)(iii) | Format and content | where applicable, description of whether the proposed remedying measures in past reviews have proven ineffective or created unexpected challenges, and how they could be improved; | 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:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 5 | | IAO-05 |
| Article 27.2(k)(iii) | Format and content | where applicable, description of whether the proposed remedying measures in past reviews have proven ineffective or created unexpected challenges, and how they could be improved; | 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:<br>(1) Assessments;<br>(2) Audits; and/or<br>(3) Incidents. | 3 | | RSK-06.1 |
| Article 27.2(l) | Format and content | sources of information used in the preparation of the report, including at least all of the following: | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 5 | | GOV-17 |
| Article 27.2(l)(i) | Format and content | for financial entities referred to in Article 6(6), of Regulation (EU) 2022/2554, results from internal audit; | 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 |
| Article 27.2(l)(ii) | Format and content | results from compliance assessments; | Functional | Intersects With | Conformity Monitoring | CPL-05 | Mechanisms exist to validate that Technology Assets, Applications, Services and/or Data (TAASD) conform to the organization's security, compliance and/or resilience policies, standards and other applicable requirements. | 5 | | CPL-03 |
| Article 27.2(l)(iii) | Format and content | results from digital operational resilience testing and, where applicable, advanced testing of ICT tools, systems and processes based on TLPT; | Functional | Intersects With | Contingency Plan Testing & Exercises | BCD-10 | Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan. | 3 | | BCD-04 |
| Article 27.2(l)(iii) | Format and content | results from digital operational resilience testing and, where applicable, advanced testing of ICT tools, systems and processes based on TLPT; | Functional | Intersects With | Penetration Testing | VPM-18 | Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS). | 5 | | VPM-07 |
| Article 27.2(l)(iv) | Format and content | external sources. | Functional | Intersects With | Security, Compliance & Resilience Status Reporting | CPL-27 | Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required. | 3 | | GOV-17 |
| Title III | Simplified ICT Risk Management Framework for Financial Entities Referred to in Article 16(1) of Regulation (EU) 2022/2554 | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Title III - Chapter I | Simplified ICT Risk Management Framework | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 28.1 | Governance and organisation | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk to achieve a high level of digital operational resilience. | 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 |
| Article 28.1 | Governance and organisation | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk to achieve a high level of digital operational resilience. | 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 |
| Article 28.2 | Governance and organisation | As part of their ICT risk management framework, the financial entities referred to in paragraph 1 shall ensure that their management body: | 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 |

**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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 28.2 | Governance and organisation | As part of their ICT risk management framework, the financial entities referred to in paragraph 1 shall ensure that their management body: | Functional | Intersects With | Steering Committee & Program Oversight | GOV-09 | Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis. | 5 | | GOV-01.1 |
| Article 28.2(a) | Governance and organisation | bears the overall responsibility for ensuring that the ICT risk management framework enables the achievement of the financial entity's business strategy in accordance with its risk appetite and ensures that ICT risk is considered in this context; | 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 |
| Article 28.2(a) | Governance and organisation | bears the overall responsibility for ensuring that the ICT risk management framework enables the achievement of the financial entity's business strategy in accordance with its risk appetite and ensures that ICT risk is considered in this context; | Functional | Intersects With | Steering Committee & Program Oversight | GOV-09 | Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis. | 5 | | GOV-01.1 |
| Article 28.2(a) | Governance and organisation | bears the overall responsibility for ensuring that the ICT risk management framework enables the achievement of the financial entity's business strategy in accordance with its risk appetite and ensures that ICT risk is considered in this context; | 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 |
| Article 28.2(b) | Governance and organisation | sets clear roles and responsibilities for all ICT-related tasks; | 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). | 8 | | GOV-04 |
| Article 28.2(b) | Governance and organisation | sets clear roles and responsibilities for all ICT-related tasks; | Functional | Intersects With | Defined Roles & Responsibilities | HRS-04 | Mechanisms exist to define cybersecurity roles & responsibilities for all personnel. | 5 | | HRS-03 |
| Article 28.2(c) | Governance and organisation | sets out information security objectives and ICT requirements; | 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 |
| Article 28.2(c) | Governance and organisation | sets out information security objectives and ICT requirements; | Functional | Intersects With | Steering Committee & Program Oversight | GOV-09 | Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis. | 3 | | GOV-01.1 |
| Article 28.2(d) | Governance and organisation | approves, oversees and periodically reviews the financial entity's: | Functional | Intersects With | Steering Committee & Program Oversight | GOV-09 | Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis. | 5 | | GOV-01.1 |
| Article 28.2(d)(i) | Governance and organisation | classification of information assets referred to in Article 30 paragraph 1, list of main risks identified, business impact analysis and related policies; | 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 |
| Article 28.2(d)(i) | Governance and organisation | classification of information assets referred to in Article 30 paragraph 1, list of main risks identified, business impact analysis and related policies; | 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 |
| Article 28.2(d)(i) | Governance and organisation | classification of information assets referred to in Article 30 paragraph 1, list of main risks identified, business impact analysis and related policies; | 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 |
| Article 28.2(d)(ii) | Governance and organisation | business continuity plans and response and recovery measures referred to in Article 16(1), point (f), of Regulation (EU) 2022/2554; | 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:<br>(1) Routine operations; and<br>(2) Adverse conditions. | 5 | | BCD-01 |
| Article 28.2(d)(ii) | Governance and organisation | business continuity plans and response and recovery measures referred to in Article 16(1), point (f), of Regulation (EU) 2022/2554; | Functional | Intersects With | Steering Committee & Program Oversight | GOV-09 | Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis. | 3 | | GOV-01.1 |
| Article 28.2(e) | Governance and organisation | allocates and reviews at least yearly the appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training and ICT skills for all staff; | 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. | 8 | | PRM-03 |
| Article 28.2(e) | Governance and organisation | allocates and reviews at least yearly the appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training and ICT skills for all staff; | 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 |
| Article 28.2(f) | Governance and organisation | defines and implements the policy and the measures included in Chapters I, II and III of this Title to identify, assess and manage the ICT risk the financial entity is exposed to; | 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 |
| Article 28.2(f) | Governance and organisation | defines and implements the policy and the measures included in Chapters I, II and III of this Title to identify, assess and manage the ICT risk the financial entity is exposed to; | 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:<br>(1) The organization's Enterprise Risk Management (ERM); and<br>(2) Industry-recognized cybersecurity risk management practices. | 5 | | RSK-01 |
| Article 28.2(g) | Governance and organisation | identifies and implements procedures, ICT protocols and tools that are necessary to protect all information assets and ICT assets; | Functional | Intersects With | Operationalizing Security, Compliance & Resilience Capabilities | GOV-11 | Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control. | 5 | | GOV-15 |
| Article 28.2(g) | Governance and organisation | identifies and implements procedures, ICT protocols and tools that are necessary to protect all information assets and ICT assets; | Functional | Intersects With | Operations Security | OPS-02 | Mechanisms exist to facilitate the implementation of operational security controls. | 5 | | OPS-01 |
| Article 28.2(h) | Governance and organisation | ensures that the staff of the financial entity is kept up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, commensurate to the ICT risk being managed; | 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 |
| Article 28.2(h) | Governance and organisation | ensures that the staff of the financial entity is kept up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, commensurate to the ICT risk being managed; | 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 |
| Article 28.2(i) | Governance and organisation | establishes reporting arrangements, including the frequency, form and content of reporting to the management body on the information security and digital operational resilience. | 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 |
| Article 28.3 | Governance and organisation | Financial entities referred to in paragraph 1 may, in accordance with Union and national sectoral law, outsource the tasks of verifying compliance with ICT risk management requirements to ICT intra-group or ICT third-party service providers. In case of such outsourcing, the financial entity remains fully responsible for the verification of compliance with the ICT risk management requirements. | Functional | Intersects With | Third-Party Management | TPM-02 | Mechanisms exist to facilitate the implementation of third-party management controls. | 5 | | TPM-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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 28.3 | Governance and organisation | Financial entities referred to in paragraph 1 may, in accordance with Union and national sectoral law, outsource the tasks of verifying compliance with ICT risk management requirements to ICT intra-group or ICT third-party service providers. In case of such outsourcing, the financial entity remains fully responsible for the verification of compliance with the ICT risk management requirements. | 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 |
| Article 28.4 | Governance and organisation | Financial entities referred to in paragraph 1 shall ensure appropriate segregation and independence of control functions and internal audit functions. | 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 |
| Article 28.4 | Governance and organisation | Financial entities referred to in paragraph 1 shall ensure appropriate segregation and independence of control functions and internal audit functions. | 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 |
| Article 28.5 | Governance and organisation | Financial entities referred to in paragraph 1 shall ensure that their ICT risk management framework is subject to an internal audit by auditors, in line with the financial entities' audit plan. The auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity. | Functional | Intersects With | Internal Audit Function | CPL-07.1 | Mechanisms exist to implement an internal audit function that is capable of providing executive management with insights into the overall management of the organization's security, compliance and resilience capabilities. | 8 | | CPL-02.1 |
| Article 28.5 | Governance and organisation | Financial entities referred to in paragraph 1 shall ensure that their ICT risk management framework is subject to an internal audit by auditors, in line with the financial entities' audit plan. The auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity. | 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 |
| Article 28.5 | Governance and organisation | Financial entities referred to in paragraph 1 shall ensure that their ICT risk management framework is subject to an internal audit by auditors, in line with the financial entities' audit plan. The auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity. | Functional | Intersects With | Assessment Team Subject Matter Expertise | CPL-09 | Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable:<br>(1) Professional qualifications to perform the audit and/or assessment; and<br>(2) Subject matter expertise to perform review, interview and test activities for in-scope People, Processes, Technologies, Data and/or Facilities (PPTDF). | 3 | | CPL-01.6 |
| Article 28.6 | Governance and organisation | Based on the outcome of the audit referred to in paragraph 5, financial entities referred to in paragraph 1 shall ensure the timely verification and remediation of critical ICT audit findings. | 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 |
| Article 28.6 | Governance and organisation | Based on the outcome of the audit referred to in paragraph 5, financial entities referred to in paragraph 1 shall ensure the timely verification and remediation of critical ICT audit findings. | 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:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 3 | | IAO-05 |
| Article 29.1 | Information security policy and measures | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop, document and implement an information security policy in the context of the ICT risk management framework. The information security policy shall define the high-level principles and rules to protect the confidentiality, integrity, availability and authenticity of data and of the services financial entities provide. | 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 |
| Article 29.2 | Information security policy and measures | Based on their information security policy, financial entities referred to in paragraph 1 shall establish and implement ICT security measures to mitigate their exposure to ICT risk, including mitigating measures implemented by ICT third-party service providers. | 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 |
| Article 29.2 | Information security policy and measures | Based on their information security policy, financial entities referred to in paragraph 1 shall establish and implement ICT security measures to mitigate their exposure to ICT risk, including mitigating measures implemented by ICT third-party service providers. | Functional | Intersects With | Risk Remediation | RSK-17 | Mechanisms exist to remediate risks to an acceptable level. | 3 | | RSK-06 |
| Article 29.2 | Information security policy and measures | Based on their information security policy, financial entities referred to in paragraph 1 shall establish and implement ICT security measures to mitigate their exposure to ICT risk, including mitigating measures implemented by ICT third-party service providers. | Functional | Intersects With | Third-Party Management | TPM-02 | Mechanisms exist to facilitate the implementation of third-party management controls. | 3 | | TPM-01 |
| Article 29.3 | Information security policy and measures | The ICT security measures shall include all of the measures referred to in Articles 30 to 38. | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 30.1 | Classification of information assets and ICT assets | As part of the ICT risk management framework referred to in Article 16(1), point (a), of Regulation (EU) 2022/2554, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall identify, classify and document all critical or important functions, the information assets and ICT assets supporting them and their interdependencies. Financial entities shall review the identification and classification as needed. | Functional | Intersects With | Asset Inventories | AST-04 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel. | 5 | | AST-02 |
| Article 30.1 | Classification of information assets and ICT assets | As part of the ICT risk management framework referred to in Article 16(1), point (a), of Regulation (EU) 2022/2554, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall identify, classify and document all critical or important functions, the information assets and ICT assets supporting them and their interdependencies. Financial entities shall review the identification and classification as | 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 |
| Article 30.1 | Classification of information assets and ICT assets | As part of the ICT risk management framework referred to in Article 16(1), point (a), of Regulation (EU) 2022/2554, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall identify, classify and document all critical or important functions, the information assets and ICT assets supporting them and their interdependencies. Financial entities shall review the identification and classification as | 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 |
| Article 30.2 | Classification of information assets and ICT assets | Financial entities referred to in paragraph 1 shall identify all critical or important functions supported by ICT third-party service providers. | 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 |
| Article 30.2 | Classification of information assets and ICT assets | Financial entities referred to in paragraph 1 shall identify all critical or important functions supported by ICT third-party service providers. | Functional | Intersects With | Third-Party Criticality Assessments | TPM-09 | Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services. | 5 | | TPM-02 |
| Article 31.1 | ICT risk management | The ICT risk management framework of financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall include all of the following elements relating to the ICT management: | 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:<br>(1) The organization's Enterprise Risk Management (ERM); and<br>(2) Industry-recognized cybersecurity risk management practices. | 5 | | RSK-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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 31.1(a) | ICT risk management | determination of the risk tolerance levels for ICT risk, in accordance with the risk appetite of the financial entity; | 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 |
| Article 31.1(b) | ICT risk management | identification and assessment of the ICT risks to which the financial entity is exposed; | Functional | Intersects With | Risk Identification | RSK-09 | Mechanisms exist to identify and document risks, both internal and external. | 5 | | RSK-03 |
| Article 31.1(b) | ICT risk management | identification and assessment of the ICT risks to which the financial entity 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 |
| Article 31.1(c) | ICT risk management | definition of mitigation strategies at least for the ICT risk that are not within the risk tolerance levels of the financial entity; | Functional | Subset Of | Risk Remediation | RSK-17 | Mechanisms exist to remediate risks to an acceptable level. | 10 | | RSK-06 |
| Article 31.1(d) | ICT risk management | monitoring the effectiveness of the mitigation strategies referred to in point (c); | 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 |
| Article 31.1(d) | ICT risk management | monitoring the effectiveness of the mitigation strategies referred to in point (c); | Functional | Intersects With | Risk Monitoring | RSK-22 | Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including:<br>(1) The effectiveness of security, compliance and resilience controls;<br>(2) Changes to the organization's risk profile; and<br>(3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk. | 5 | | RSK-11 |
| Article 31.1(e) | ICT risk management | identification and assessment of any ICT and information security risks resulting from any major change in ICT system or ICT services, processes or procedures, as well as from ICT security testing results and after any major ICT-related incident. | 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 |
| Article 31.1(e) | ICT risk management | identification and assessment of any ICT and information security risks resulting from any major change in ICT system or ICT services, processes or procedures, as well as from ICT security testing results and after any major ICT-related incident. | 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 |
| Article 31.2 | ICT risk management | The ICT risk assessment shall be carried out and documented periodically commensurate to the financial entities' ICT risk profile. | 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 |
| Article 31.3 | ICT risk management | Financial entities referred to in paragraph 1 shall ensure that they continuously monitor threats and vulnerabilities relevant to their critical or important functions, supporting information and ICT assets and shall 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:<br>(1) The effectiveness of security, compliance and resilience controls;<br>(2) Changes to the organization's risk profile; and<br>(3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk. | 3 | | RSK-11 |
| Article 31.3 | ICT risk management | Financial entities referred to in paragraph 1 shall ensure that they continuously monitor threats and vulnerabilities relevant to their critical or important functions, supporting information and ICT assets and shall 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 |
| Article 31.3 | ICT risk management | Financial entities referred to in paragraph 1 shall ensure that they continuously monitor threats and vulnerabilities relevant to their critical or important functions, supporting information and ICT assets and shall 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 |
| Article 31.4 | ICT risk management | Financial entities referred to in paragraph 1 shall define alert thresholds and criteria to trigger and initiate ICT-related incident response processes. | Functional | Intersects With | Incident Handling | IRO-06 | Mechanisms exist to cover:<br>(1) Preparation;<br>(2) Automated event detection or manual incident report intake;<br>(3) Analysis;<br>(4) Containment;<br>(5) Eradication; and<br>(6) Recovery. | 3 | | IRO-02 |
| Article 31.4 | ICT risk management | Financial entities referred to in paragraph 1 shall define alert thresholds and criteria to trigger and initiate ICT-related incident response processes. | Functional | Intersects With | Alert Threshold Tuning | MON-07 | Mechanisms exist to "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events. | 5 | | MON-01.13 |
| Article 32.1 | Physical and environmental security | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall identify and implement physical security measures designed according to the threat landscape and to the classification referred to in Article 30 paragraph 1 and overall risk profile of ICT assets and information assets that can be accessed. | Functional | Intersects With | Physical & Environmental Protections | PES-02 | Mechanisms exist to facilitate the operation of physical and environmental protection controls. | 8 | | PES-01 |
| Article 32.2 | Physical and environmental security | The measures referred to in paragraph 1 shall protect the premises and, where applicable, data centres of the financial entity where ICT assets and information assets reside from unauthorised access, attacks, accidents and from environmental threats and hazards. | Functional | Intersects With | Physical & Environmental Protections | PES-02 | Mechanisms exist to facilitate the operation of physical and environmental protection controls. | 5 | | PES-01 |
| Article 32.2 | Physical and environmental security | The measures referred to in paragraph 1 shall protect the premises and, where applicable, data centres of the financial entity where ICT assets and information assets reside from unauthorised access, attacks, accidents and from environmental threats and hazards. | 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 |
| Article 32.3 | Physical and environmental security | The protection from environmental threats and hazards shall be commensurate with the importance of the premises and, where applicable, the data centres and the criticality of the operations or ICT systems located there. | Functional | Intersects With | Physical & Environmental Protections | PES-02 | Mechanisms exist to facilitate the operation of physical and environmental protection controls. | 5 | | PES-01 |
| Article 32.3 | Physical and environmental security | The protection from environmental threats and hazards shall be commensurate with the importance of the premises and, where applicable, the data centres and the criticality of the operations or ICT systems located there. | Functional | Intersects With | Supporting Utilities | PES-20 | Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction. | 5 | | PES-07 |
| Title III - Chapter II | Further Elements of Systems, Protocols, and Tools to Minimise the Impact of ICT Risk | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 33.1 | Access Control | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall define, document and implement procedures for logical and physical access control and shall enforce, monitor and periodically review these procedures. These procedures shall define the following logical and physical access control elements: | 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 |
| Article 33.1 | Access Control | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall define, document and implement procedures for logical and physical access control and shall enforce, monitor and periodically review these procedures. These procedures shall define the following logical and physical access control elements: | 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 |
| Article 33.1(a) | Access Control | access rights to information assets, ICT assets and their supported functions, critical locations of operation of the financial entity shall be managed on a need-to-know, need-to- use and least privileges basis, including for remote and emergency access; | Functional | Intersects With | Access Enforcement | IAC-25 | Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege." | 5 | | IAC-20 |
| Article 33.1(a) | Access Control | access rights to information assets, ICT assets and their supported functions, critical locations of operation of the financial entity shall be managed on a need-to-know, need-to- use and least privileges basis, including for remote and emergency access; | Functional | Intersects With | Least Privilege | IAC-30 | Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business | 8 | | IAC-21 |
| Article 33.1(b) | Access Control | user accountability, thereby ensuring 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. | 5 | | IAC-15.5 |
| Article 33.1(b) | Access Control | user accountability, thereby ensuring 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 |

**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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 33.1(c) | Access Control | account management procedures to grant, change or revoke access rights for user and generic accounts, including generic administrator accounts. Privileged, emergency and administrator access shall be assigned on a need-to-use or an ad-hoc basis for all ICT systems and shall be logged in accordance with Article 34(1), point (f); | Functional | Intersects With | Account Management | IAC-08 | Mechanisms exist to:<br>(1) Define authorized system account types;<br>(2) Define prohibited system account types; and<br>(3) Proactively govern individual, group, system, service, application, guest and temporary accounts. | 8 | | IAC-15 |
| Article 33.1(c) | Access Control | account management procedures to grant, change or revoke access rights for user and generic accounts, including generic administrator accounts. Privileged, emergency and administrator access shall be assigned on a need-to-use or an ad-hoc basis for all ICT systems and shall be logged in accordance with Article 34(1), point (f); | Functional | Intersects With | Privileged Account Management (PAM) | IAC-10 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 5 | | IAC-16 |
| Article 33.1(c) | Access Control | account management procedures to grant, change or revoke access rights for user and generic accounts, including generic administrator accounts. Privileged, emergency and administrator access shall be assigned on a need-to-use or an ad-hoc basis for all ICT systems and shall be logged in accordance with Article 34(1), point (f); | Functional | Intersects With | Privileged Functions Logging | MON-14 | Mechanisms exist to log and review the actions of users and/or services with elevated privileges. | 3 | | MON-03.3 |
| Article 33.1(d) | Access Control | the use of authentication methods commensurate to the classification referred to in Article 30 paragraph 1 and overall risk profile of ICT assets and considering leading practices. | Functional | Intersects With | Authenticator Management | IAC-14 | Mechanisms exist to:<br>(1) Securely manage authenticators for users and devices; and<br>(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed. | 5 | | IAC-10 |
| Article 33.1(d) | Access Control | the use of authentication methods commensurate to the classification referred to in Article 30 paragraph 1 and overall risk profile of ICT assets and considering leading practices. | 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 |
| Article 33.1(e) | Access Control | The use of strong authentication methods in accordance with leading practices for remote access to the financial entities' network, for privileged access, and for access to ICT assets supporting critical or important functions that are publicly available; | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-37 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:<br>(1) Remote network access;<br>(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or<br>(3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data. | 8 | | IAC-06 |
| Article 33.1(e) | Access Control | The use of strong authentication methods in accordance with leading practices for remote access to the financial entities' network, for privileged access, and for access to ICT assets supporting critical or important functions that are publicly available; | 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 |
| Article 33.1(e) | Access Control | The use of strong authentication methods in accordance with leading practices for remote access to the financial entities' network, for privileged access, and for access to ICT assets supporting critical or important functions that are publicly available; | Functional | Intersects With | Remote Access | NET-26 | Mechanisms exist to define, control and review organization-approved, secure remote access methods. | 3 | | NET-14 |
| Article 33.1(f) | Access Control | access rights shall be periodically reviewed and shall be 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 |
| Article 34.1 | ICT operations security | As part of their systems, protocols and tools, and for all ICT assets, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall: | Functional | Intersects With | Operations Security | OPS-02 | Mechanisms exist to facilitate the implementation of operational security controls. | 5 | | OPS-01 |
| Article 34.1(a) | ICT operations security | monitor and manage the life cycle of these ICT assets to ensure that they continue to meet and support business and risk management requirements; | Functional | Intersects With | Asset Inventories | AST-04 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:<br>(1) Accurately reflects the current TAASD in use;<br>(2) Identifies authorized software products, including business justification details;<br>(3) Is at the level of granularity deemed necessary for tracking and reporting;<br>(4) Includes organization-defined information deemed necessary to achieve effective property accountability; and<br>(5) Is available for review and audit by designated organizational personnel. | 5 | | AST-02 |
| Article 34.1(a) | ICT operations security | monitor and manage the life cycle of these ICT assets to ensure that they continue to meet and support business and risk management requirements; | 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 |
| Article 34.1(b) | ICT operations security | monitor whether these ICT assets are supported by their ICT third-party service providers, if applicable; | Functional | Intersects With | Technology Lifecycle Management | AST-37 | Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS). | 3 | | SEA-07.1 |
| Article 34.1(b) | ICT operations security | monitor whether these ICT assets are supported by their ICT third-party service providers, if applicable; | 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:<br>(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and<br>(2) Requiring justification and documented approval for the continued use of unsupported TAAS required | 5 | | TDA-17 |
| Article 34.1(c) | ICT operations security | identify capacity requirements of their ICT systems and measures to maintain and improve the availability and efficiency of ICT systems and prevent ICT capacity shortages before they materialise; | 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 |
| Article 34.1(c) | ICT operations security | identify capacity requirements of their ICT systems and measures to maintain and improve the availability and efficiency of ICT systems and prevent ICT capacity shortages before they materialise; | 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 |
| Article 34.1(d) | ICT operations security | perform automated vulnerability scanning and assessments of ICT assets commensurate to their classification referred to in Article 30 paragraph 1 and overall risk profile of the ICT asset, and deploy patches to address identified vulnerabilities; | Functional | Intersects With | Vulnerability Remediation Process | VPM-06 | Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated. | 3 | | VPM-02 |
| Article 34.1(d) | ICT operations security | perform automated vulnerability scanning and assessments of ICT assets commensurate to their classification referred to in Article 30 paragraph 1 and overall risk profile of the ICT asset, and deploy patches to address identified vulnerabilities; | 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 |
| Article 34.1(d) | ICT operations security | perform automated vulnerability scanning and assessments of ICT assets commensurate to their classification referred to in Article 30 paragraph 1 and overall risk profile of the ICT asset, and deploy patches to address identified vulnerabilities; | Functional | Intersects With | Vulnerability Scanning | VPM-12 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | | VPM-06 |
| Article 34.1(e) | ICT operations security | manage the risks related to outdated or unsupported and legacy ICT assets; | 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 |
| Article 34.1(e) | ICT operations security | manage the risks related to outdated or unsupported and legacy ICT assets; | 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:<br>(1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and<br>(2) Requiring justification and documented approval for the continued use of unsupported TAAS required | 8 | | TDA-17 |
| Article 34.1(f) | ICT operations security | log events related to logical and physical access control, ICT operations, including system and network traffic activities, ICT change management. The level of detail of the logs shall be aligned with their purpose and usage of the ICT asset producing the logs; | Functional | Intersects With | Continuous Monitoring | MON-02 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 5 | | MON-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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 34.1(f) | ICT operations security | log events related to logical and physical access control, ICT operations, including system and network traffic activities, ICT change management. The level of detail of the logs shall be aligned with their purpose and usage of the ICT asset producing the logs; | Functional | Intersects With | Content of Event Logs | MON-09 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:<br>(1) Establish what type of event occurred;<br>(2) When (date and time) the event occurred;<br>(3) Where the event occurred;<br>(4) The source of the event;<br>(5) The outcome (success or failure) of the event; and<br>(6) The identity of any user/subject associated with the event. | 5 | | MON-03 |
| Article 34.1(g) | ICT operations security | identify and implement measures to monitor and analyse information on anomalous activities and behaviour for critical or important ICT operations; | Functional | Intersects With | Continuous Monitoring | MON-02 | Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls. | 5 | | MON-01 |
| Article 34.1(g) | ICT operations security | identify and implement measures to monitor and analyse information on anomalous activities and behaviour for critical or important ICT operations; | 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. | 8 | | MON-16 |
| Article 34.1(h) | ICT operations security | implement measures to monitor relevant and up-to-date information about cyber 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. | 8 | | THR-01 |
| Article 34.1(h) | ICT operations security | implement measures to monitor relevant and up-to-date information about cyber threats; | Functional | Intersects With | Threat Intelligence Feeds | THR-04 | Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls. | 5 | | THR-03 |
| Article 34.1(i) | ICT operations security | implement measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and shall 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. | 5 | | END-04 |
| Article 34.1(i) | ICT operations security | implement measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and shall 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 |
| Article 34.1(i) | ICT operations security | implement measures to identify possible information leakages, malicious code and other security threats, and publicly known vulnerabilities in software and hardware and shall check for corresponding new security updates. | 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 |
| Article 35.1 | Data, system and network security | As part of their systems, protocols and tools, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop and implement safeguards to ensure the security of networks against intrusions and data misuse and to preserve the availability, authenticity, integrity and confidentiality of data and shall establish all of the following taking into account the classification performed pursuant to Article 30(1): | Functional | Intersects With | Data Protection | DCH-02 | Mechanisms exist to facilitate the implementation of data protection controls. | 3 | | DCH-01 |
| Article 35.1 | Data, system and network security | As part of their systems, protocols and tools, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop and implement safeguards to ensure the security of networks against intrusions and data misuse and to preserve the availability, authenticity, integrity and confidentiality of data and shall establish all of the following taking into account the classification performed pursuant to Article 30(1): | Functional | Intersects With | Network Security Controls (NSC) | NET-02 | Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC). | 5 | | NET-01 |
| Article 35.1(a) | Data, system and network security | measures to protect data in use, in transit and at rest; | Functional | Intersects With | Encrypting Data In Transit | CRY-05 | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit. | 5 | | CRY-03 |
| Article 35.1(a) | Data, system and network security | measures to protect data in use, in transit and at rest; | Functional | Intersects With | Encrypting Data At Rest | CRY-07 | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest. | 5 | | CRY-05 |
| Article 35.1(a) | Data, system and network security | measures to protect data in use, in transit and at rest; | Functional | Intersects With | Data Protection | DCH-02 | Mechanisms exist to facilitate the implementation of data protection controls. | 3 | | DCH-01 |
| Article 35.1(b) | Data, system and network security | identification of security measures regarding the use of software, data storage media, systems and endpoint devices transferring and storing data of the financial entity; | Functional | Intersects With | Digital Media Use Restrictions | DCH-19 | Mechanisms exist to restrict the use of types of digital media on systems or system components. | 5 | | DCH-10 |
| Article 35.1(b) | Data, system and network security | identification of security measures regarding the use of software, data storage media, systems and endpoint devices transferring and storing data of the financial entity; | Functional | Intersects With | Endpoint Protection Mechanisms | END-03 | Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices. | 5 | | END-02 |
| Article 35.1(c) | Data, system and network security | identification and implementation of measures to prevent and detect unauthorised connections to the financial entity's network and to secure the network traffic between the financial entity's internal networks and the internet and other external connections; | Functional | Intersects With | Boundary Protection | NET-03 | Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network. | 8 | | NET-03 |
| Article 35.1(c) | Data, system and network security | identification and implementation of measures to prevent and detect unauthorised connections to the financial entity's network and to secure the network traffic between the financial entity's internal networks and the internet and other external connections; | Functional | Intersects With | Network Intrusion Detection / Prevention Systems (NIDS / NIPS) | NET-31 | Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network. | 5 | | NET-08 |
| Article 35.1(d) | Data, system and network security | identification of measures ensuring the availability, authenticity, integrity and confidentiality of data during network transmission; | Functional | Intersects With | Encrypting Data In Transit | CRY-05 | Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit. | 5 | | CRY-03 |
| Article 35.1(d) | Data, system and network security | identification of measures ensuring the availability, authenticity, integrity and confidentiality of data during network transmission; | Functional | Intersects With | Integrity of Data In Transit | CRY-06 | Cryptographic mechanisms exist to detect unauthorized changes to data in transit. | 5 | | CRY-04 |
| Article 35.1(e) | Data, system and network security | process to securely delete data on premises or stored externally that the financial entity no longer needs to collect or store; | Functional | Intersects With | Digital & Non-Digital Media Disposal | DCH-17 | Mechanisms exist to securely dispose of, destroy and/or erase digital and non-digital media when it is no longer required, using organization-defined procedures. | 8 | | DCH-21 |
| Article 35.1(e) | Data, system and network security | process to securely delete data on premises or stored externally that the financial entity no longer needs to collect or store; | Functional | Intersects With | Digital Media Sanitization | DCH-18 | Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse. | 5 | | DCH-09 |
| Article 35.1(f) | Data, system and network security | process to securely dispose of or decommission data storage devices on premises or stored externally containing confidential information; | Functional | Intersects With | Secure Disposal, Destruction or Re-Use of Equipment | AST-22 | Mechanisms exist to securely dispose of, destroy or repurpose technology assets using organization-defined techniques and methods to prevent:<br>(1) Data recovery; and<br>(2) Components from being resold, redistributed and/or reused through unauthorized channels. | 8 | | AST-09 |
| Article 35.1(f) | Data, system and network security | process to securely dispose of or decommission data storage devices on premises or stored externally containing confidential information; | Functional | Intersects With | Digital Media Sanitization | DCH-18 | Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse. | 5 | | DCH-09 |
| Article 35.1(g) | Data, system and network security | the implementation of measures to ensure that teleworking and the use of private endpoint devices does not adversely impact the financial entity's ability to carry out its critical activities in an adequate, timely and secure manner. | Functional | Intersects With | Use of Personal Devices | AST-25 | Mechanisms exist to restrict the possession and/or use of personally-owned Technology Assets, Applications and/or Services (TAAS) within organization-controlled facilities. | 5 | | AST-12 |
| Article 35.1(g) | Data, system and network security | the implementation of measures to ensure that teleworking and the use of private endpoint devices does not adversely impact the financial entity's ability to carry out its critical activities in an adequate, timely and secure manner. | Functional | Intersects With | Work From Anywhere (WFA) - Telecommuting Security | NET-27 | Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers. | 5 | | NET-14.5 |
| Article 36.1 | ICT security testing | For the purposes of Article 16(3), first subparagraph, point (d), of Regulation (EU) 2022/2554, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall establish and implement an ICT security testing plan to validate the effectiveness of their ICT security measures developed in accordance with Articles 33 to 35 and 37 to 38, and ensure that this plan considers threats and vulnerabilities identified as part of the ICT risk management framework referred to in Article 31(3). | 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 |

**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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 36.1 | ICT security testing | For the purposes of Article 16(3), first subparagraph, point (d), of Regulation (EU) 2022/2554, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall establish and implement an ICT security testing plan to validate the effectiveness of their ICT security measures developed in accordance with Articles 33 to 35 and 37 to 38, and ensure that this plan considers threats and vulnerabilities identified as part of the ICT risk management framework referred to in Article 31(3). | 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 |
| Article 36.1 | ICT security testing | For the purposes of Article 16(3), first subparagraph, point (d), of Regulation (EU) 2022/2554, financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall establish and implement an ICT security testing plan to validate the effectiveness of their ICT security measures developed in accordance with Articles 33 to 35 and 37 to 38, and ensure that this plan considers threats and vulnerabilities identified as part of the ICT risk management framework referred to in Article 31(3). | 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 |
| Article 36.2 | ICT security testing | Financial entities referred to in paragraph 1 shall ensure that reviews, assessments and tests of ICT security measures are conducted taking into consideration the overall risk profile of the financial entity. | 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 |
| Article 36.2 | ICT security testing | Financial entities referred to in paragraph 1 shall ensure that reviews, assessments and tests of ICT security measures are conducted taking into consideration the overall risk profile of the financial entity. | 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 |
| Article 36.3 | ICT security testing | Financial entities referred to in paragraph 1 shall monitor and evaluate the results of the security tests and update their security measures accordingly without undue delay in the case of ICT systems supporting critical or important functions. | 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:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 5 | | IAO-05 |
| Article 36.3 | ICT security testing | Financial entities referred to in paragraph 1 shall monitor and evaluate the results of the security tests and update their security measures accordingly without undue delay in the case of ICT systems supporting critical or important functions. | Functional | Intersects With | Risk Remediation | RSK-17 | Mechanisms exist to remediate risks to an acceptable level. | 3 | | RSK-06 |
| Article 37.1 | ICT systems acquisition, development and maintenance | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall design and implement, where appropriate, a procedure governing the acquisition, development and maintenance of ICT systems following a risk-based approach. The procedure governing the acquisition, development and maintenance of ICT systems shall: | 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 |
| Article 37.1 | ICT systems acquisition, development and maintenance | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall design and implement, where appropriate, a procedure governing the acquisition, development and maintenance of ICT systems following a risk-based approach. The procedure governing the acquisition, development and maintenance of ICT systems shall: | 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 |
| Article 37.1(a) | ICT systems acquisition, development and maintenance | 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 function; | Functional | Intersects With | Security, Compliance & Resilience Requirements Definition | PRM-09 | Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by:<br>(1) Defining technical security, compliance and resilience requirements; and<br>(2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC). | 8 | | PRM-05 |
| Article 37.1(a) | ICT systems acquisition, development and maintenance | 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 function; | 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 |
| Article 37.1(b) | ICT systems acquisition, development and maintenance | ensure the testing and approval of ICT systems prior to their first use and before introducing changes to 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. | 5 | | CHG-02.2 |
| Article 37.1(b) | ICT systems acquisition, development and maintenance | ensure the testing and approval of ICT systems prior to their first use and before introducing changes to 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. | 3 | | IAO-07 |
| Article 37.1(b) | ICT systems acquisition, development and maintenance | ensure the testing and approval of ICT systems prior to their first use and before introducing changes to 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:<br>(1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability;<br>(2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and | 8 | | TDA-09 |
| Article 37.1(c) | ICT systems acquisition, development and maintenance | identify measures 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 |
| Article 37.1(c) | ICT systems acquisition, development and maintenance | identify measures 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 |
| Article 38.1 | ICT project and change management | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop, document and implement an ICT project management procedure and define the roles and responsibilities for its implementation. The ICT project management procedure shall cover all stages of the ICT projects from their initiation to closure. | 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 |
| Article 38.1 | ICT project and change management | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop, document and implement an ICT project management procedure and define the roles and responsibilities for its implementation. The ICT project management procedure shall cover all stages of the ICT projects from their initiation to closure. | 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 |
| Article 38.2 | ICT project and change management | Financial entities referred to in paragraph 1 shall develop, document and implement an ICT change management procedure to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner and with the adequate safeguards to preserve the financial entity's digital operational resilience. | Functional | Intersects With | Change Management Program | CHG-02 | Mechanisms exist to facilitate the implementation of a change management program. | 8 | | CHG-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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 38.2 | ICT project and change management | Financial entities referred to in paragraph 1 shall develop, document and implement an ICT change management procedure to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner and with the adequate safeguards to preserve the financial entity's digital operational resilience. | Functional | Intersects With | Configuration Change Control | CHG-03 | Mechanisms exist to govern the technical configuration change control processes. | 5 | | CHG-02 |
| Title III - Chapter III | ICT Business Continuity | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Title II - Chapter IV | ICT Business Continuity Management | N/A | 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:<br>(1) Routine operations; and | 10 | | BCD-01 |
| Article 39.1 | Components of the ICT business continuity plan | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop their ICT business continuity plans considering the results of the analysis of their exposures to and potential impact of severe business disruptions and scenarios to which their ICT assets supporting critical or important functions might be exposed, including a cyber-attack scenario. | Functional | Intersects With | Identify Critical Assets | AST-05 | Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions. | 3 | | BCD-02 |
| Article 39.1 | Components of the ICT business continuity plan | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop their ICT business continuity plans considering the results of the analysis of their exposures to and potential impact of severe business disruptions and scenarios to which their ICT assets supporting critical or important functions might be exposed, including a cyber-attack scenario. | 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:<br>(1) Routine operations; and<br>(2) Adverse conditions. | 5 | | BCD-01 |
| Article 39.1 | Components of the ICT business continuity plan | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop their ICT business continuity plans considering the results of the analysis of their exposures to and potential impact of severe business disruptions and scenarios to which their ICT assets supporting critical or important functions might be exposed, including a cyber-attack scenario. | 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 |
| Article 39.2 | Components of the ICT business continuity plan | The ICT business continuity plans shall: | 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 |
| Article 39.2(a) | Components of the ICT business continuity plan | be approved by the management body of the financial entity; | 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 |
| Article 39.2(a) | Components of the ICT business continuity plan | be approved by the management body of the financial entity; | Functional | Intersects With | Steering Committee & Program Oversight | GOV-09 | Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis. | 3 | | GOV-01.1 |
| Article 39.2(b) | Components of the ICT business continuity plan | be documented and readily accessible in the event of an emergency or crisis; | 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 |
| Article 39.2(c) | Components of the ICT business continuity plan | allocate sufficient resources to execute the plan; | 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. | 3 | | BCD-01.7 |
| Article 39.2(c) | Components of the ICT business continuity plan | allocate sufficient resources to execute the plan; | 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 |
| Article 39.2(d) | Components of the ICT business continuity plan | establish planned recovery levels and timeframes for the recovery and resumption of functions and key internal and external dependencies including ICT third-party service providers; | 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 |
| Article 39.2(d) | Components of the ICT business continuity plan | establish planned recovery levels and timeframes for the recovery and resumption of functions and key internal and external dependencies including ICT third-party service providers; | Functional | Intersects With | Third-Party Incident Response & Recovery Capabilities | TPM-21 | Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers. | 3 | | TPM-11 |
| Article 39.2(e) | Components of the ICT business continuity plan | identify the conditions that may prompt the activation of the plans and what actions shall be taken to ensure the availability, continuity and recovery of the financial entities' ICT assets supporting critical or important functions; | 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 |
| Article 39.2(e) | Components of the ICT business continuity plan | identify the conditions that may prompt the activation of the plans and what actions shall be taken to ensure the availability, continuity and recovery of the financial entities' ICT assets supporting critical or important functions; | 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 |
| Article 39.2(f) | Components of the ICT business continuity plan | identify the restoration and recovery measures for critical or important business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of the financial entities. These measures shall include the mitigation of failures of critical third-party providers as well; | 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 |
| Article 39.2(f) | Components of the ICT business continuity plan | identify the restoration and recovery measures for critical or important business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of the financial entities. These measures shall include the mitigation of failures of critical third-party providers as well; | 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 |
| Article 39.2(f) | Components of the ICT business continuity plan | identify the restoration and recovery measures for critical or important business functions, supporting processes, information assets and their interdependencies to avoid adverse effects on the functioning of the financial entities. These measures shall include the mitigation of failures of critical third-party providers as well; | Functional | Intersects With | Third-Party Incident Response & Recovery Capabilities | TPM-21 | Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers. | 3 | | TPM-11 |
| Article 39.2(g) | Components of the ICT business continuity plan | identify backup procedures and measures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup based on the criticality of the function using those data; | Functional | Intersects With | Data Backups | BCD-24 | Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 8 | | BCD-11 |
| Article 39.2(g) | Components of the ICT business continuity plan | identify backup procedures and measures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup based on the criticality of the function using those data; | Functional | Intersects With | Testing for Reliability & Integrity | BCD-32 | Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data. | 5 | | BCD-11.1 |
| Article 39.2(h) | Components of the ICT business continuity plan | 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 |
| Article 39.2(h) | Components of the ICT business continuity plan | 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 |
| Article 39.2(i) | Components of the ICT business continuity plan | specify the internal and external communication arrangements including escalation plans; | 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 |

**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:** EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)
**Focal Document URL:** https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
**Published STRM URL:** https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 39.2(i) | Components of the ICT business continuity plan | specify the internal and external communication arrangements including escalation plans; | Functional | Intersects With | Incident Stakeholder Reporting | IRO-16 | Mechanisms exist to timely-report incidents to applicable:<br>(1) Internal stakeholders;<br>(2) Affected clients & third-parties; and<br>(3) Regulatory authorities. | 5 | | IRO-10 |
| Article 39.2(j) | Components of the ICT business continuity plan | be updated in line with lessons learned from incidents, tests, new risks and threats identified, changed recovery objectives, major changes to the financial entity's organisation and to the ICT assets supporting critical or business functions. | Functional | Intersects With | Ongoing Contingency Planning | BCD-07 | Mechanisms exist to update contingency plans due to changes affecting:<br>(1) People (e.g., personnel changes);<br>(2) Processes (e.g., new, altered or decommissioned business practices, including third-party services);<br>(3) Technologies (e.g., new, altered or decommissioned technologies);<br>(4) Data (e.g., changes to data flows and/or data repositories);<br>(5) Facilities (e.g., new, altered or decommissioned physical infrastructure); and/or<br>(6) Feedback from contingency plan testing | 5 | | BCD-06 |
| Article 39.2(j) | Components of the ICT business continuity plan | be updated in line with lessons learned from incidents, tests, new risks and threats identified, changed recovery objectives, major changes to the financial entity's organisation and to the ICT assets supporting critical or business functions. | 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 |
| Article 40.1 | Testing of business continuity plans | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall test their business continuity plans referred to in Article 39, including the scenarios defined in Article 39(1) at least once every year for the back-up and restore procedures or upon every major change of the business continuity plan. | 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 |
| Article 40.1 | Testing of business continuity plans | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall test their business continuity plans referred to in Article 39, including the scenarios defined in Article 39(1) at least once every year for the back-up and restore procedures or upon every major change of the business continuity plan. | 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 |
| Article 40.2 | Testing of business continuity plans | The testing of their business continuity plans shall demonstrate that the financial entities referred to in paragraph 1 are able to sustain the viability of their businesses until critical operations are re-established and identify any deficiencies in the business continuity plan. | 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. | 3 | | BCD-02.2 |
| Article 40.2 | Testing of business continuity plans | The testing of their business continuity plans shall demonstrate that the financial entities referred to in paragraph 1 are able to sustain the viability of their businesses until critical operations are re-established and identify any deficiencies in the business continuity plan. | 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 |
| Article 40.3 | Testing of business continuity plans | Financial entities referred to in paragraph 1 shall document the test results of the testing of business continuity plans and any identified deficiencies resulting from the tests should be analysed, addressed and reported to the management body. | 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 |
| Article 40.3 | Testing of business continuity plans | Financial entities referred to in paragraph 1 shall document the test results of the testing of business continuity plans 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 |
| Article 40.3 | Testing of business continuity plans | Financial entities referred to in paragraph 1 shall document the test results of the testing of business continuity plans 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 |
| Title III - Chapter IV | Report on the Review of the ICT Risk Management Framework | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 41.1 | Format and content | Financial entities referred to in Article 16(1) of Regulation (EU) 2022/2554 shall develop and document the report referred to in Article 16(2) of Regulation (EU) 2022/2554 in a searchable electronic format. | 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 |
| Article 41.2 | Format and content | The report shall include all of the following information: | 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 |
| Article 41.2(a) | Format and content | an introductory section providing: | 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 |
| Article 41.2(a)(i) | Format and content | a description of the context of the report in terms of the nature, scale and complexity of the financial entity's services, activities and operations, its organisation, identified critical functions, strategy, major ongoing projects or activities, relationships and its dependence on in-house and outsourced ICT services and systems or the implications that a total loss or severe degradation of such systems would have on critical or important functions and market efficiency; | 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 |
| Article 41.2(a)(ii) | Format and content | an executive level summary of the current and near-term ICT risk identified, threat landscape, the assessed effectiveness of its controls and the security posture of the financial entity; | 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 |
| Article 41.2(a)(iii) | Format and content | information about the reported area; | 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 |
| Article 41.2(a)(iv) | Format and content | a list of major changes which were done in the reported area; | 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 |
| Article 41.2(a)(v) | Format and content | a summary and a description of the impact of major changes to the ICT risk management framework since the previous report; | 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 |
| Article 41.2(b) | Format and content | where applicable, date of the approval of the report by the management body of the financial entity; | 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 |
| Article 41.2(c) | Format and content | a description of the reasons for the review, including: | 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 |
| Article 41.2(c)(i) | Format and content | in case the review has been initiated following supervisory instructions, evidence of such instructions; | 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 |
| Article 41.2(c)(ii) | Format and content | in case the review has been initiated following the occurrence of ICT-related incidents, the list of all ICT-related incidents with related incident root-cause analysis; | 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 |

**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: **EU - DORA Draft RTS on ICT Risk Management Framework and on Simplified ICT Risk Management Framework (JC 2023 86)**
Focal Document URL: https://www.esma.europa.eu/sites/default/files/2024-01/JC_2023_86_-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-eu-dora-rts-2024.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 # |
|---|---|---|---|---|---|---|---|---|---|---|
| Article 41.2(c)(ii) | Format and content | in case the review has been initiated following the occurrence of ICT-related incidents, the list of all ICT-related incidents with related incident root-cause analysis; | Functional | Intersects With | Root Cause Analysis (RCA) & Lessons Learned | IRO-14 | Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents. | 5 | | IRO-13 |
| Article 41.2(d) | Format and content | start and end date of the review period; | 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 |
| Article 41.2(e) | Format and content | the person responsible for the review; | 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 |
| Article 41.2(f) | Format and content | a summary of findings and a self-assessment of the severity of the weaknesses, deficiencies and gaps identified in ICT risk management framework for the review period, including a detailed analysis thereof; | 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 |
| Article 41.2(f) | Format and content | a summary of findings and a self-assessment of the severity of the weaknesses, deficiencies and gaps identified in ICT risk management framework for the review period, including a detailed analysis thereof; | 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 |
| Article 41.2(g) | Format and content | remedying measures identified to address weaknesses, deficiencies and gaps in the ICT risk management framework and expected date for implementing these measures including the follow-up on weaknesses, deficiencies and gaps identified in previous reports, if they have not been remedied; | 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. | 3 | | CPL-02.3 |
| Article 41.2(g) | Format and content | remedying measures identified to address weaknesses, deficiencies and gaps in the ICT risk management framework and expected date for implementing these measures including the follow-up on weaknesses, deficiencies and gaps identified in previous reports, if they have not been remedied; | 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:<br>(1) Deficiency tracking number;<br>(2) Applicable security, compliance and/or resilience control;<br>(3) Description of the deficiency(ies);<br>(4) Risk associated with the deficiency(ies);<br>(5) Source deficiency identification/detection;<br>(6) Temporary compensating controls, if applicable;<br>(7) Point of Contact (POC) (e.g., asset/process owner);<br>(8) Resources required to conduct remediation actions;<br>(9) Planned remedial actions to the deficiency(ies);<br>(10) Proposed remediation timeline; and<br>(11) Disposition statement (e.g., closeout summary). | 5 | | IAO-05 |
| Article 41.2(h) | Format and content | overall conclusions on the review of the ICT risk management framework, including any further planned developments. | 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 |
| Title IV | Final Provisions | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Title IV - Chapter I | Final Provisions | N/A | Functional | No Relationship | N/A | N/A | N/A | 0 | | |
| Article 42 | Entry into force | This Regulation shall enter into force on the 20th day following its publication in the Official Journal of the European Union. This Regulation shall be binding in its entirety and directly applicable in all Member States. Done at Brussels, XX XXXX XXXX For the Commission The President | Functional | No Relationship | N/A | N/A | N/A | 0 | | |