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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
org.1	Security Policy	ISO 27002:2022 5.1 Information security policies	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
org.1	Security Policy	ISO 27002:2022 5.1 Information security policies	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
org.1	Security Policy	ISO 27002:2022 5.1 Information security policies	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
org.1	Security Policy	ISO 27002:2022 5.1 Information security policies	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
org.1	Security Policy	ISO 27002:2022 5.1 Information security policies	Functional	Intersects With	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	5	
org.2	Security regulations	ISO 27002:2022 5.1 Information security policies	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
org.2	Security regulations	ISO 27002:2022 5.1 Information security policies	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
org.2	Security regulations	ISO 27002:2022 5.1 Information security policies	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
org.2	Security regulations	ISO 27002:2022 5.1 Information security policies	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
org.2	Security regulations	ISO 27002:2022 5.1 Information security policies	Functional	Intersects With	Dissemination of Data Privacy Program Information	PRI-01.3	Mechanisms exist to: (1) Ensure that the public has access to information about organizational data privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; (2) Ensure that organizational data privacy practices are publicly available through organizational websites or document repositories; (3) Utilize publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to data privacy office(s) regarding data privacy practices; and (4) Inform data subjects when changes are made to the privacy notice and the nature of such changes.	5	
org.3	Security procedures	ISO 27002:2022 5.37 Documentation of operational procedures	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
org.3	Security procedures	ISO 27002:2022 5.37 Documentation of operational procedures	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
org.3	Security procedures	ISO 27002:2022 5.37 Documentation of operational procedures	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
org.3	Security procedures	ISO 27002:2022 5.37 Documentation of operational procedures	Functional	Subset Of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	
org.3	Security procedures	ISO 27002:2022 5.37 Documentation of operational procedures	Functional	Equal	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
org.3	Security procedures	ISO 27002:2022 5.37 Documentation of operational procedures	Functional	Intersects With	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
org.4	Authorisation process	ISO 27002:2022 5.2 Roles and responsibilities in information security	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	5	
org.4	Authorisation process	ISO 27002:2022 5.2 Roles and responsibilities in information security	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
org.4	Authorisation process	ISO 27002:2022 5.2 Roles and responsibilities in information security	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
org.4	Authorisation process	ISO 27002:2022 5.2 Roles and responsibilities in information security	Functional	Intersects With	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for security, compliance and resilience controls between internal stakeholders and External Service Providers (ESPs).	5	
org.4	Authorisation process	ISO 27002:2022 5.2 Roles and responsibilities in information security	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
op.pl.1	Risk analysis	ISO 27002:2022 6.1 Actions to address risks and opportunities	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
op.pl.1	Risk analysis	ISO 27002:2022 6.1 Actions to address risks and opportunities	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive and/or regulated data is stored, transmitted or processed.	5	
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	5	
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5	
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).	5	
op.pl.2	Security architecture	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and	5	
op.pl.3	Acquisition of new components	ISO 27002:2022 5.8 Information security in project management	Functional	Subset Of	Security, Compliance & Resilience Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of resource planning controls that provide a portfolio management approach to achieve security, compliance and resilience objectives.	10	
op.pl.3	Acquisition of new components	ISO 27002:2022 5.8 Information security in project management	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	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	
op.pl.3	Acquisition of new components	ISO 27002:2022 5.8 Information security in project management	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and	5	
op.pl.3	Acquisition of new components	ISO 27002:2022 5.8 Information security in project management	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	
op.pl.3	Acquisition of new components	ISO 27002:2022 5.8 Information security in project management	Functional	Intersects With	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
op.pl.3	Acquisition of new components	ISO 27002:2022 5.8 Information security in project management	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
op.pl.3	Acquisition of new components	ISO 27002:2022 5.8 Information security in project management	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
op.pl.3	Acquisition of new components	ISO 27002:2022 5.8 Information security in project management	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
op.pl.3	Acquisition of new components	ISO 27002:2022 5.8 Information security in project management	Functional	Intersects With	Risk Response	RSK-06.1	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.	5	
op.pl.3	Acquisition of new components	ISO 27002:2022 5.8 Information security in project management	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
op.pl.4	Dimensioning / Capacity Management	ISO 27002:2022 8.6 Capacity Management	Functional	Subset Of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
op.pl.4	Dimensioning / Capacity Management	ISO 27002:2022 8.6 Capacity Management	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	
op.pl.5	Certified components	No compatible measures	Functional	No Relationship	N/A	N/A	N/A	0	
op.acc.1	Identification	ISO 27002:2022 5.16 Identity management	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
op.acc.1	Identification	ISO 27002:2022 5.16 Identity management	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
op.acc.1	Identification	ISO 27002:2022 5.16 Identity management	Functional	Intersects With	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	5	
op.acc.1	Identification	ISO 27002:2022 5.16 Identity management	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
op.acc.1	Identification	ISO 27002:2022 5.16 Identity management	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	5	
op.acc.1	Identification	ISO 27002:2022 5.16 Identity management	Functional	Intersects With	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	
op.acc.1	Identification	ISO 27002:2022 5.16 Identity management	Functional	Intersects With	Cross-Organization Management	IAC-09.4	Mechanisms exist to coordinate username identifiers with external organizations for cross-organization management of identifiers.	5	
op.acc.1	Identification	ISO 27002:2022 5.16 Identity management	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and	5	
op.acc.1	Identification	ISO 27002:2022 5.16 Identity management	Functional	Intersects With	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5	
op.acc.1	Identification	ISO 27002:2022 5.16 Identity management	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and	5	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Physical Access Authorizations	PES-02	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	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
op.acc.2	Access requirements	ISO 27002:2022 5.15 Access control	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	
op.acc.3	Segregation of roles and tasks	ISO 27002:2022 5.3 Segregation of duties	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
op.acc.3	Segregation of roles and tasks	ISO 27002:2022 5.3 Segregation of duties	Functional	Intersects With	Incompatible Roles	HRS-12	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	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Removal of Temporary / Emergency Accounts	IAC-15.2	Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-20.1	Mechanisms exist to limit access to sensitive and/or regulated data to only those individuals whose job requires such access.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Database Access	IAC-20.2	Mechanisms exist to restrict access to databases containing sensitive and/or regulated data to only necessary Technology Assets, Applications and/or Services (TAAS) or those individuals whose job requires such access.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Use of Privileged Utility Programs	IAC-20.3	Mechanisms exist to restrict and tightly control utility programs that are capable of overriding system and application controls.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Physical Access Authorizations	PES-02	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	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	
op.acc.4	Access rights management process	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and	5	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Removal of Temporary / Emergency Accounts	IAC-15.2	Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-20.1	Mechanisms exist to limit access to sensitive and/or regulated data to only those individuals whose job requires such access.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Database Access	IAC-20.2	Mechanisms exist to restrict access to databases containing sensitive and/or regulated data to only necessary Technology Assets, Applications and/or Services (TAAS) or those individuals whose job requires such access.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Use of Privileged Utility Programs	IAC-20.3	Mechanisms exist to restrict and tightly control utility programs that are capable of overriding system and application controls.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Management Approval For Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Physical Access Authorizations	PES-02	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	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	
op.acc.5	Authentication mechanism (external users)	ISO 27002:2022 5.18 Access rights	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
op.acc.6	Authentication mechanism (users of the organisation)	ISO 27002:2022 8.5 Secure authentication	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
op.acc.6	Authentication mechanism (users of the organisation)	ISO 27002:2022 8.5 Secure authentication	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
op.acc.6	Authentication mechanism (users of the organisation)	ISO 27002:2022 8.5 Secure authentication	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
op.acc.6	Authentication mechanism (users of the organisation)	ISO 27002:2022 8.5 Secure authentication	Functional	Intersects With	Trusted Path	END-09	Mechanisms exist to establish a trusted communications path between the user and the security functions of the operating system.	5	
op.acc.6	Authentication mechanism (users of the organisation)	ISO 27002:2022 8.5 Secure authentication	Functional	Intersects With	Secure Log-On Procedures	SEA-17	Mechanisms exist to utilize a trusted communications path between the user and the security functions of the system.	5	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive and/or regulated data is stored, transmitted or processed.	5	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	5	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).	5	
op.exp.1	Inventory of assets	ISO 27002:2022 5.9 Inventory of information and other associated assets	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and	5	
op.exp.2	Security settings	ISO 27002:2022 8.9 Configuration management	Functional	Subset Of	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	10	
op.exp.2	Security settings	ISO 27002:2022 8.9 Configuration management	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
op.exp.2	Security settings	ISO 27002:2022 8.9 Configuration management	Functional	Intersects With	Assignment of Responsibility	CFG-01.1	Mechanisms exist to implement a segregation of duties for configuration management that prevents developers from performing production configuration management duties.	5	
op.exp.2	Security settings	ISO 27002:2022 8.9 Configuration management	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
op.exp.2	Security settings	ISO 27002:2022 8.9 Configuration management	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
op.exp.2	Security settings	ISO 27002:2022 8.9 Configuration management	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
op.exp.3	Configuration management	ISO 27002:2022 8.9 Configuration management	Functional	Subset Of	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	10	
op.exp.3	Configuration management	ISO 27002:2022 8.9 Configuration management	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
op.exp.3	Configuration management	ISO 27002:2022 8.9 Configuration management	Functional	Intersects With	Assignment of Responsibility	CFG-01.1	Mechanisms exist to implement a segregation of duties for configuration management that prevents developers from performing production configuration management duties.	5	
op.exp.3	Configuration management	ISO 27002:2022 8.9 Configuration management	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
op.exp.3	Configuration management	ISO 27002:2022 8.9 Configuration management	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
op.exp.3	Configuration management	ISO 27002:2022 8.9 Configuration management	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
op.exp.4	Maintenance and security updates	ISO 27002:2022 7.13 Equipment maintenance	Functional	Subset Of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
op.exp.4	Maintenance and security updates	ISO 27002:2022 7.13 Equipment maintenance	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	5	
op.exp.4	Maintenance and security updates	ISO 27002:2022 7.13 Equipment maintenance	Functional	Intersects With	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	5	
op.exp.5	Change management	ISO 27002:2022 8.32 Change management	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
op.exp.5	Change management	ISO 27002:2022 8.32 Change management	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
op.exp.5	Change management	ISO 27002:2022 8.32 Change management	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	
op.exp.5	Change management	ISO 27002:2022 8.32 Change management	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	
op.exp.5	Change management	ISO 27002:2022 8.32 Change management	Functional	Intersects With	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	5	
op.exp.6	Protection against malicious code	ISO 27002:2022 8.7 Controls against malicious code	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
op.exp.6	Protection against malicious code	ISO 27002:2022 8.7 Controls against malicious code	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
op.exp.7	Incident management	ISO 27002:2022 5.24 Information Security Incident Management Planning and Preparedness	Functional	Subset Of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
op.exp.7	Incident management	ISO 27002:2022 5.24 Information Security Incident Management Planning and Preparedness	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
op.exp.7	Incident management	ISO 27002:2022 5.24 Information Security Incident Management Planning and Preparedness	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
op.exp.7	Incident management	ISO 27002:2022 5.24 Information Security Incident Management Planning and Preparedness	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
op.exp.8	Logging of user activity	ISO 27002:2022 8.15 Event registration	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
op.exp.8	Logging of user activity	ISO 27002:2022 8.15 Event registration	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
op.exp.8	Logging of user activity	ISO 27002:2022 8.15 Event registration	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
op.exp.8	Logging of user activity	ISO 27002:2022 8.15 Event registration	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
op.exp.8	Logging of user activity	ISO 27002:2022 8.15 Event registration	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	
op.exp.8	Logging of user activity	ISO 27002:2022 8.15 Event registration	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
op.exp.8	Logging of user activity	ISO 27002:2022 8.15 Event registration	Functional	Intersects With	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	
op.exp.8	Logging of user activity	ISO 27002:2022 8.15 Event registration	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
op.exp.8	Logging of user activity	ISO 27002:2022 8.15 Event registration	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
op.exp.9	Incident management record	ISO 27002:2022 5.26 Information security incident response	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
op.exp.9	Incident management record	ISO 27002:2022 5.26 Information security incident response	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
op.exp.9	Incident management record	ISO 27002:2022 5.26 Information security incident response	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
op.exp.9	Incident management record	ISO 27002:2022 5.26 Information security incident response	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	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	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)
Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
op.exp.10	Cryptographic key protection	ISO 27002:2022 8.24 Use of cryptography	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
op.exp.10	Cryptographic key protection	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
op.exp.10	Cryptographic key protection	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
op.exp.10	Cryptographic key protection	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
op.exp.10	Cryptographic key protection	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
op.exp.10	Cryptographic key protection	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
op.exp.10	Cryptographic key protection	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	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	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
op.ext.1	Contracting and service level agreements	ISO 27002:2022 5.19 Information security in supplier relations	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
op.ext.2	Day-to-day management	ISO 27002:2022 5.22 Monitoring, Review and Change Management of Supplier Services	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
op.ext.2	Day-to-day management	ISO 27002:2022 5.22 Monitoring, Review and Change Management of Supplier Services	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5	
op.ext.2	Day-to-day management	ISO 27002:2022 5.22 Monitoring, Review and Change Management of Supplier Services	Functional	Intersects With	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	5	
op.ext.2	Day-to-day management	ISO 27002:2022 5.22 Monitoring, Review and Change Management of Supplier Services	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
op.ext.2	Day-to-day management	ISO 27002:2022 5.22 Monitoring, Review and Change Management of Supplier Services	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	
op.ext.3	Supply chain security	ISO 27002:2022 5.21 Information security management in the ICT supply chain	Functional	Intersects With	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to Technology Assets, Applications, Services and/or Data (TAASD).	5	
op.ext.3	Supply chain security	ISO 27002:2022 5.21 Information security management in the ICT supply chain	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
op.ext.3	Supply chain security	ISO 27002:2022 5.21 Information security management in the ICT supply chain	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
op.ext.3	Supply chain security	ISO 27002:2022 5.21 Information security management in the ICT supply chain	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or	5	
op.ext.3	Supply chain security	ISO 27002:2022 5.21 Information security management in the ICT supply chain	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
op.ext.3	Supply chain security	ISO 27002:2022 5.21 Information security management in the ICT supply chain	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
op.ext.3	Supply chain security	ISO 27002:2022 5.21 Information security management in the ICT supply chain	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique Technology Assets, Applications and/or Services (TAAS).	5	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
op.ext.3	Supply chain security	ISO 27002:2022 5.21 Information security management in the ICT supply chain	Functional	Intersects With	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	
op.ext.3	Supply chain security	ISO 27002:2022 5.21 Information security management in the ICT supply chain	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
op.ext.3	Supply chain security	ISO 27002:2022 5.21 Information security management in the ICT supply chain	Functional	Intersects With	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization utilizes.	5	
op.ext.4	System interconnection	ISO 27002:2022 8.22 Segregation in networks	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5	
op.ext.4	System interconnection	ISO 27002:2022 8.22 Segregation in networks	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.	5	
op.ext.4	System interconnection	ISO 27002:2022 8.22 Segregation in networks	Functional	Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	5	
op.nub.1	Protection of cloud services	No compatible measures	Functional	Subset Of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
op.cont.1	Impact analysis	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
op.cont.1	Impact analysis	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
op.cont.1	Impact analysis	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	5	
op.cont.1	Impact analysis	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	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	
op.cont.1	Impact analysis	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
op.cont.1	Impact analysis	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Coordination with Related Plans	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	5	
op.cont.1	Impact analysis	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5	
op.cont.2	Continuity plan	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
op.cont.2	Continuity plan	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
op.cont.2	Continuity plan	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	5	
op.cont.2	Continuity plan	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	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	
op.cont.2	Continuity plan	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5	
op.cont.2	Continuity plan	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Coordination with Related Plans	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	5	
op.cont.2	Continuity plan	ISO 27002:2022 5.29 Information Security During Disruption	Functional	Intersects With	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.	5	
op.cont.3	Periodic tests	ISO 27002:2022 5.30 ICT Preparedness for Business Continuity	Functional	Intersects With	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
op.cont.3	Periodic tests	ISO 27002:2022 5.30 ICT Preparedness for Business Continuity	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5	
op.cont.3	Periodic tests	ISO 27002:2022 5.30 ICT Preparedness for Business Continuity	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
op.cont.3	Periodic tests	ISO 27002:2022 5.30 ICT Preparedness for Business Continuity	Functional	Intersects With	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
op.cont.3	Periodic tests	ISO 27002:2022 5.30 ICT Preparedness for Business Continuity	Functional	Intersects With	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	5	
op.cont.3	Periodic tests	ISO 27002:2022 5.30 ICT Preparedness for Business Continuity	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	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	
op.cont.3	Periodic tests	ISO 27002:2022 5.30 ICT Preparedness for Business Continuity	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
op.cont.3	Periodic tests	ISO 27002:2022 5.30 ICT Preparedness for Business Continuity	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	
op.cont.4	Alternative means	ISO 27002:2022 8.14 Redundancy of information processing resources	Functional	Intersects With	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	5	
op.cont.4	Alternative means	ISO 27002:2022 8.14 Redundancy of information processing resources	Functional	Intersects With	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5	
op.cont.4	Alternative means	ISO 27002:2022 8.14 Redundancy of information processing resources	Functional	Intersects With	Redundant Secondary System	BCD-11.7	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.	5	
op.mon.1	Intrusion detection	ISO 27002:2022 8.20 Network security	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5	
op.mon.1	Intrusion detection	ISO 27002:2022 8.20 Network security	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
op.mon.1	Intrusion detection	ISO 27002:2022 8.20 Network security	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
op.mon.1	Intrusion detection	ISO 27002:2022 8.20 Network security	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
op.mon.1	Intrusion detection	ISO 27002:2022 8.20 Network security	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	
op.mon.1	Intrusion detection	ISO 27002:2022 8.20 Network security	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
op.mon.1	Intrusion detection	ISO 27002:2022 8.20 Network security	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
op.mon.1	Intrusion detection	ISO 27002:2022 8.20 Network security	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	
op.mon.2	Metric system	ISO 27002:2022 9 Performance evaluation	Functional	Intersects With	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5	
op.mon.2	Metric system	ISO 27002:2022 9 Performance evaluation	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor Security, Compliance & Resilience Program (SCRP) measures of performance.	5	
op.mon.2	Metric system	ISO 27002:2022 9 Performance evaluation	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
op.mon.2	Metric system	ISO 27002:2022 9 Performance evaluation	Functional	Intersects With	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
op.mon.2	Metric system	ISO 27002:2022 9 Performance evaluation	Functional	Intersects With	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	8	
op.mon.2	Metric system	ISO 27002:2022 9 Performance evaluation	Functional	Intersects With	Control Conformity Monitoring	CPL-03	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	
op.mon.3	Surveillance	ISO 27002:2022 5.7 Threat intelligence	Functional	Intersects With	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	5	
op.mon.3	Surveillance	ISO 27002:2022 5.7 Threat intelligence	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
op.mon.3	Surveillance	ISO 27002:2022 5.7 Threat intelligence	Functional	Subset Of	Threat Intelligence Program	THR-01	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.	10	
op.mon.3	Surveillance	ISO 27002:2022 5.7 Threat intelligence	Functional	Intersects With	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
op.mon.3	Surveillance	ISO 27002:2022 5.7 Threat intelligence	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
op.mon.3	Surveillance	ISO 27002:2022 5.7 Threat intelligence	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	5	
mp.if.1	Separate and access-controlled areas	ISO 27002:2022 7.1 Physical security perimeter	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
mp.if.1	Separate and access-controlled areas	ISO 27002:2022 7.1 Physical security perimeter	Functional	Intersects With	Physical Access Authorizations	PES-02	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	
mp.if.1	Separate and access-controlled areas	ISO 27002:2022 7.1 Physical security perimeter	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
mp.if.1	Separate and access-controlled areas	ISO 27002:2022 7.1 Physical security perimeter	Functional	Intersects With	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	5	
mp.if.1	Separate and access-controlled areas	ISO 27002:2022 7.1 Physical security perimeter	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
mp.if.2	Identification of persons	ISO 27002:2022 7.2 Physical input controls	Functional	Intersects With	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	5	
mp.if.2	Identification of persons	ISO 27002:2022 7.2 Physical input controls	Functional	Intersects With	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	
mp.if.2	Identification of persons	ISO 27002:2022 7.2 Physical input controls	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	
mp.if.2	Identification of persons	ISO 27002:2022 7.2 Physical input controls	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
mp.if.2	Identification of persons	ISO 27002:2022 7.2 Physical input controls	Functional	Intersects With	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	5	
mp.if.3	Fitting-out of premises	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
mp.if.3	Fitting-out of premises	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
mp.if.3	Fitting-out of premises	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
mp.if.3	Fitting-out of premises	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned	10	
mp.if.3	Fitting-out of premises	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
mp.if.4	Electrical energy	ISO 27002:2022 7.11 Supply installations	Functional	Intersects With	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5	
mp.if.4	Electrical energy	ISO 27002:2022 7.11 Supply installations	Functional	Intersects With	Automatic Voltage Controls	PES-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	5	
mp.if.4	Electrical energy	ISO 27002:2022 7.11 Supply installations	Functional	Intersects With	Emergency Shutoff	PES-07.2	Facility security mechanisms exist to shut off power in emergency situations by: (1) Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and (2) Protecting emergency power shutoff capability from unauthorized activation.	5	
mp.if.4	Electrical energy	ISO 27002:2022 7.11 Supply installations	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	5	
mp.if.4	Electrical energy	ISO 27002:2022 7.11 Supply installations	Functional	Intersects With	Emergency Lighting	PES-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	5	
mp.if.5	Fire protection	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
mp.if.5	Fire protection	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
mp.if.5	Fire protection	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
mp.if.5	Fire protection	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned	10	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
mp.if.5	Fire protection	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
mp.if.6	Protection against floods	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
mp.if.6	Protection against floods	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
mp.if.6	Protection against floods	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Intersects With	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	5	
mp.if.6	Protection against floods	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned	10	
mp.if.6	Protection against floods	ISO 27002:2022 7.5 Protection against external and environmental threats	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
mp.if.7	Equipment input and output register	ISO 27002:2022 7.2 Physical input controls	Functional	Intersects With	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	5	
mp.if.7	Equipment input and output register	ISO 27002:2022 7.2 Physical input controls	Functional	Intersects With	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	
mp.if.7	Equipment input and output register	ISO 27002:2022 7.2 Physical input controls	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	
mp.if.7	Equipment input and output register	ISO 27002:2022 7.2 Physical input controls	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
mp.if.7	Equipment input and output register	ISO 27002:2022 7.2 Physical input controls	Functional	Intersects With	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.	5	
mp.per.1	Job characterisation	ISO 27002:2022 6.1 Checking	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
mp.per.1	Job characterisation	ISO 27002:2022 6.1 Checking	Functional	Intersects With	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
mp.per.2	Duties and obligations	Terms and conditions of engagement	Functional	No Relationship	N/A	N/A	N/A	0	
mp.per.3	Awareness raising	ISO 27002:2022 6.3 Information security awareness, education and training	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
mp.per.3	Awareness raising	ISO 27002:2022 6.3 Information security awareness, education and training	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
mp.per.3	Awareness raising	ISO 27002:2022 6.3 Information security awareness, education and training	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
mp.per.4	Training	ISO 27002:2022 6.3 Information security awareness, education and training	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
mp.per.4	Training	ISO 27002:2022 6.3 Information security awareness, education and training	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
mp.per.4	Training	ISO 27002:2022 6.3 Information security awareness, education and training	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
mp.eq.1	Clear workstation	ISO 27002:2022 7.7 Uncluttered workstation and clean screen	Functional	Intersects With	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and unauthorized access.	5	
mp.eq.1	Clear workstation	ISO 27002:2022 7.7 Uncluttered workstation and clean screen	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
mp.eq.1	Clear workstation	ISO 27002:2022 7.7 Uncluttered workstation and clean screen	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
mp.eq.2	Locking of the workstation	ISO 27002:2022 7.7 Uncluttered workstation and clean screen	Functional	Intersects With	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and unauthorized access.	5	
mp.eq.2	Locking of the workstation	ISO 27002:2022 7.7 Uncluttered workstation and clean screen	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
mp.eq.2	Locking of the workstation	ISO 27002:2022 7.7 Uncluttered workstation and clean screen	Functional	Intersects With	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
mp.eq.3	Portable equipment protection	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and unauthorized access.	5	
mp.eq.3	Portable equipment protection	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive and/or regulated data via direct physical interaction from tampering and substitution.	5	
mp.eq.3	Portable equipment protection	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Use of Personal Devices	AST-12	Mechanisms exist to restrict the possession and/or use of personally-owned Technology Assets, Applications and/or Services (TAAS) within organization-controlled facilities.	5	
mp.eq.3	Portable equipment protection	ISO 27002:2022 8.1 User end devices	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
mp.eq.3	Portable equipment protection	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
mp.eq.3	Portable equipment protection	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	
mp.eq.3	Portable equipment protection	ISO 27002:2022 8.1 User end devices	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
mp.eq.3	Portable equipment protection	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	5	
mp.eq.3	Portable equipment protection	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	5	
mp.eq.4	Other network connected devices	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and unauthorized access.	5	
mp.eq.4	Other network connected devices	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Kiosks & Point of Interaction (PoI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive and/or regulated data via direct physical interaction from tampering and substitution.	5	
mp.eq.4	Other network connected devices	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Use of Personal Devices	AST-12	Mechanisms exist to restrict the possession and/or use of personally-owned Technology Assets, Applications and/or Services (TAAS) within organization-controlled facilities.	5	
mp.eq.4	Other network connected devices	ISO 27002:2022 8.1 User end devices	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
mp.eq.4	Other network connected devices	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
mp.eq.4	Other network connected devices	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	
mp.eq.4	Other network connected devices	ISO 27002:2022 8.1 User end devices	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
mp.eq.4	Other network connected devices	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	5	
mp.eq.4	Other network connected devices	ISO 27002:2022 8.1 User end devices	Functional	Intersects With	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	5	
mp.com.1	Secure perimeter	ISO 27002:2022 8.20 Network security	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive and/or regulated data flows.	5	
mp.com.1	Secure perimeter	ISO 27002:2022 8.20 Network security	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
mp.com.1	Secure perimeter	ISO 27002:2022 8.20 Network security	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
mp.com.1	Secure perimeter	ISO 27002:2022 8.20 Network security	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
mp.com.1	Secure perimeter	ISO 27002:2022 8.20 Network security	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	
mp.com.1	Secure perimeter	ISO 27002:2022 8.20 Network security	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
mp.com.1	Secure perimeter	ISO 27002:2022 8.20 Network security	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5	
mp.com.1	Secure perimeter	ISO 27002:2022 8.20 Network security	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	
mp.com.2	Protection of confidentiality	ISO 27002:2022 8.21 Security of network services	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
mp.com.2	Protection of confidentiality	ISO 27002:2022 8.21 Security of network services	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
mp.com.2	Protection of confidentiality	ISO 27002:2022 8.21 Security of network services	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
mp.com.2	Protection of confidentiality	ISO 27002:2022 8.21 Security of network services	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
mp.com.2	Protection of confidentiality	ISO 27002:2022 8.21 Security of network services	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
mp.com.2	Protection of confidentiality	ISO 27002:2022 8.21 Security of network services	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
mp.com.3	Authenticity and integrity protection	ISO 27002:2022 8.21 Security of network services	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
mp.com.3	Authenticity and integrity protection	ISO 27002:2022 8.21 Security of network services	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
mp.com.3	Authenticity and integrity protection	ISO 27002:2022 8.21 Security of network services	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
mp.com.3	Authenticity and integrity protection	ISO 27002:2022 8.21 Security of network services	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
mp.com.3	Authenticity and integrity protection	ISO 27002:2022 8.21 Security of network services	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
mp.com.3	Authenticity and integrity protection	ISO 27002:2022 8.21 Security of network services	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5	
mp.com.4	Separation of information flows in the network	ISO 27002:2022 8.22 Segregation in networks	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5	
mp.com.4	Separation of information flows in the network	ISO 27002:2022 8.22 Segregation in networks	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.	5	
mp.com.4	Separation of information flows in the network	ISO 27002:2022 8.22 Segregation in networks	Functional	Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized Technology Assets, Applications and/or Services (TAAS) on certain services, protocols and ports.	5	
mp.si.1	Carrier marking	ISO 27002:2022 5.13 Labelling of information	Functional	Equal	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	10	
mp.si.2	Cryptography	ISO 27002:2022 8.24 Use of cryptography	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
mp.si.2	Cryptography	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
mp.si.2	Cryptography	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
mp.si.2	Cryptography	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
mp.si.2	Cryptography	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
mp.si.2	Cryptography	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
mp.si.2	Cryptography	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Removal of Assets	AST-11	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	5	
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Use of Personal Devices	AST-12	Mechanisms exist to restrict the possession and/or use of personally-owned Technology Assets, Applications and/or Services (TAAS) within organization-controlled facilities.	5	
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5	
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Limitations on Use	DCH-10.1	Mechanisms exist to restrict the use and distribution of sensitive and/or regulated data.	5	
mp.si.3	Custody	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Removal of Assets	AST-11	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	5	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Use of Personal Devices	AST-12	Mechanisms exist to restrict the possession and/or use of personally-owned Technology Assets, Applications and/or Services (TAAS) within organization-controlled facilities.	5	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Limitations on Use	DCH-10.1	Mechanisms exist to restrict the use and distribution of sensitive and/or regulated data.	5	
mp.si.4	Transport	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Removal of Assets	AST-11	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	5	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Use of Personal Devices	AST-12	Mechanisms exist to restrict the possession and/or use of personally-owned Technology Assets, Applications and/or Services (TAAS) within organization-controlled facilities.	5	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	5	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Limitations on Use	DCH-10.1	Mechanisms exist to restrict the use and distribution of sensitive and/or regulated data.	5	
mp.si.5	Deletion and destruction	ISO 27002:2022 7.10 Storage media	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	Functional	Intersects With	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	5	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	Functional	Intersects With	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	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	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	Functional	Subset Of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	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	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	Functional	Intersects With	Separation of Development, Testing and Operational Environments	TDA-08	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	
mp.sw.1	Application development	ISO 27002:2022 8.25 Security in the development lifecycle	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
mp.sw.2	Acceptance and entry into service	ISO 27002:2022 8.29 Developmental safety and acceptance testing	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
mp.sw.2	Acceptance and entry into service	ISO 27002:2022 8.29 Developmental safety and acceptance testing	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; (11) Artificial Intelligence and Autonomous Technologies (AAT); and/or	5	
mp.sw.2	Acceptance and entry into service	ISO 27002:2022 8.29 Developmental safety and acceptance testing	Functional	Intersects With	Minimum Viable Product (MVP) Security Requirements	TDA-02	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	
mp.sw.2	Acceptance and entry into service	ISO 27002:2022 8.29 Developmental safety and acceptance testing	Functional	Intersects With	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
mp.sw.2	Acceptance and entry into service	ISO 27002:2022 8.29 Developmental safety and acceptance testing	Functional	Intersects With	Criticality Analysis During Development	TDA-06.1	Mechanisms exist to require the developer of the Technology Asset, Application and/or Service (TAAS) to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
mp.sw.2	Acceptance and entry into service	ISO 27002:2022 8.29 Developmental safety and acceptance testing	Functional	Intersects With	Security, Compliance & Resilience Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with security, compliance and/or resilience personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the control testing and evaluation process; and (3) Document the results.	5	
mp.info.1	Personal data	ISO 27002:2022 5.34 Privacy and Personal Data Protection (PDP)	Functional	Subset Of	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	10	
mp.info.1	Personal data	ISO 27002:2022 5.34 Privacy and Personal Data Protection (PDP)	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
mp.info.1	Personal data	ISO 27002:2022 5.34 Privacy and Personal Data Protection (PDP)	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
mp.info.1	Personal data	ISO 27002:2022 5.34 Privacy and Personal Data Protection (PDP)	Functional	Intersects With	Purpose Specification	PRI-02.1	Mechanisms exist to ensure data privacy notices identify the purpose(s) for which Personal Data (PD) is collected, received, processed, stored, transmitted and/or shared.	5	
mp.info.2	Qualification of information	ISO 27002:2022 5.12 Classification of information	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
mp.info.2	Qualification of information	ISO 27002:2022 5.12 Classification of information	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
mp.info.2	Qualification of information	ISO 27002:2022 5.12 Classification of information	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
mp.info.2	Qualification of information	ISO 27002:2022 5.12 Classification of information	Functional	Intersects With	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive and/or regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	5	
mp.info.3	Electronic signature	ISO 27002:2022 8.24 Use of cryptography	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
mp.info.3	Electronic signature	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
mp.info.3	Electronic signature	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
mp.info.3	Electronic signature	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
mp.info.3	Electronic signature	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
mp.info.3	Electronic signature	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
mp.info.3	Electronic signature	ISO 27002:2022 8.24 Use of cryptography	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
mp.info.4	Time stamps	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
mp.info.4	Time stamps	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	5	
mp.info.4	Time stamps	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
mp.info.4	Time stamps	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
mp.info.4	Time stamps	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
mp.info.4	Time stamps	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and	5	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Spain - ICT Security Guide CCN - STIC 825 (2026)

Focal Document URL: https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/7122-ccn-stic-825-national-security-framework-27001-

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-ccn-stic-825-2026.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
mp.info.4	Time stamps	ISO 27002:2022 8.26 Application security requirements	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
mp.info.4	Time stamps	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
mp.info.4	Time stamps	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
mp.info.5	Cleaning of documents	It is not envisaged	Functional	No Relationship	N/A	N/A	N/A	0	
mp.info.6	Backups	ISO 27002:2022 8.13 Backing up information	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
mp.info.6	Backups	ISO 27002:2022 8.13 Backing up information	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
mp.info.6	Backups	ISO 27002:2022 8.13 Backing up information	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	
mp.info.6	Backups	ISO 27002:2022 8.13 Backing up information	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	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	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
mp.s.1	E-mail protection	ISO 27002:2022 5.14 Transfer of information	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
mp.s.2	Protection of web services and applications	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
mp.s.2	Protection of web services and applications	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Application Programming Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application Programming Interfaces (APIs).	5	
mp.s.2	Protection of web services and applications	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
mp.s.2	Protection of web services and applications	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
mp.s.2	Protection of web services and applications	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
mp.s.2	Protection of web services and applications	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to proactively govern Technology Assets, Applications and/or Services (TAAS) by: (1) Defining technical security, compliance and resilience requirements; and	5	
mp.s.2	Protection of web services and applications	ISO 27002:2022 8.26 Application security requirements	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
mp.s.2	Protection of web services and applications	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for security, compliance and resilience principles that addresses risk to organizational operations, assets, individuals and other organizations.	5	
mp.s.2	Protection of web services and applications	ISO 27002:2022 8.26 Application security requirements	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
mp.s.3	Web browsing protection	ISO 27002:2022 8.23 Web filtering	Functional	Equal	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
mp.s.4	Denial of service protection	ISO 27002:2022 8.6 Capacity Management	Functional	Subset Of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
mp.s.4	Denial of service protection	ISO 27002:2022 8.6 Capacity Management	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	