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 - Royal Decree 311/2022

Focal Document URL: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-decree-311-2022.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
Article 1	Purpose	This Royal Decree has as its purpose to regulate the National Security Scheme (hereinafter, ENS), established in Article 156.2 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector. The ENS consists of the basic principles and minimum requirements necessary for adequate protection of the information processed and the services provided by the entities within its scope of application, with the aim of ensuring access, confidentiality, integrity, traceability, authenticity, availability and conservation of data, information and services used by electronic means managed in the exercise of their competencies. The provisions of this Royal Decree, insofar as they affect the information systems used for the provision of public services, shall be considered within the resources and procedures forming part of the National Security System under Law 36/2015, of September 28, on National Security.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 2(1)	Scope of Application	This Royal Decree is applicable to the entire public sector, as defined in Article 2 of Law 40/2015, of October 1, and in accordance with the provisions of Article 156.2 thereof.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 2(2)	Scope of Application	Without prejudice to the application of Law 9/1968, of April 5, on Official Secrets and other special regulations, this Royal Decree shall also apply to systems that process classified information. It may be necessary to adopt complementary security measures specific to such systems, arising from international commitments entered into by Spain or its membership of international bodies or forums.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 2(3)	Scope of Application	This Royal Decree also applies to the information systems of private sector entities, including the obligation to have a security policy as referred to in Article 12, when, in accordance with applicable regulations and by virtue of a contractual relationship, they provide services or solutions to public sector entities for the exercise of their competencies and administrative powers. The security policy referred to in Article 12 shall be approved in the case of these entities by the body holding the highest executive competencies. Public procurement documentation shall include all requirements necessary to ensure ENS conformity of information systems underpinning services provided by contractors, such as the submission of corresponding ENS Declarations or Certifications of Conformity. This requirement shall also extend to the supply chain of such contractors, to the extent necessary and in accordance with the results of the corresponding risk analysis.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 2(4)	Scope of Application	When public sector entities carry out the installation, deployment and operation of 5G networks or the provision of 5G services, in addition to the provisions of this Royal Decree, the provisions of Royal Decree-Law 7/2022, of March 29, on requirements to guarantee the security of fifth-generation electronic communications networks and services shall also apply, in particular Article 17 on security management by public administrations, as well as its implementing regulations.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 3(1)	Information Systems Processing Personal Data	When an information system processes personal data, the provisions of Regulation (EU) 2016/679 (General Data Protection Regulation), Organic Law 3/2018, of December 5, on Personal Data Protection and Digital Rights Guarantee, or, where applicable, Organic Law 7/2021, of May 26, on personal data processed for purposes of prevention, detection, investigation and prosecution of criminal offences and execution of criminal sanctions, and other applicable regulations, as well as criteria established by the Spanish Data Protection Agency or regional data protection authorities, shall apply, without prejudice to the requirements established in this Royal Decree.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 3(2)	Information Systems Processing Personal Data	In such cases, the data controller or processor, advised by the data protection officer, shall carry out a risk analysis in accordance with Article 24 of the General Data Protection Regulation and, in the cases of Article 35 thereof, a data protection impact assessment.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	8	
Article 3(3)	Information Systems Processing Personal Data	In any case, the measures to be implemented as a result of the risk analysis and, where applicable, the impact assessment referred to in the preceding paragraph, shall prevail where they are more stringent than those provided for in this Royal Decree.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	3	
Article 3(3)	Information Systems Processing Personal Data	In any case, the measures to be implemented as a result of the risk analysis and, where applicable, the impact assessment referred to in the preceding paragraph, shall prevail where they are more stringent than those provided for in this Royal Decree.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
Article 4	Definitions	For the purposes of this Royal Decree, definitions, words, expressions and terms shall be understood in the sense indicated in the Glossary of terms included in Annex IV.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 5	Basic Principles of the National Security Scheme	The ultimate objective of information security is to ensure that an organisation will be able to fulfil its objectives, develop its functions and exercise its competencies using information systems. To that end, the following basic principles shall be taken into account in matters of information security:	Functional	No Relationship	N/A	N/A	N/A	0	
Article 5(a)	Basic Principles of the National Security Scheme	Security as an integral process.	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	
Article 5(b)	Basic Principles of the National Security Scheme	Risk-based security management.	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	
Article 5(c)	Basic Principles of the National Security Scheme	Prevention, detection, response and conservation.	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	
Article 5(d)	Basic Principles of the National Security Scheme	Existence of lines of defence.	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	
Article 5(e)	Basic Principles of the National Security Scheme	Continuous monitoring.	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	
Article 5(f)	Basic Principles of the National Security Scheme	Periodic reassessment.	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	
Article 5(g)	Basic Principles of the National Security Scheme	Differentiation of responsibilities.	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	
Article 6(1)	Security as an Integral Process	Security is understood as an integral process comprising all human, material, technical, legal and organisational elements related to the information system. The application of the ENS shall be governed by this principle, which excludes any ad hoc or circumstantial action.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 6(2)	Security as an Integral Process	Maximum attention shall be paid to raising awareness among the persons involved in the process and their hierarchical superiors, in order to prevent ignorance, lack of organisation and coordination, or inadequate instructions from becoming sources of security risk.	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	
Article 7(1)	Risk-Based Security Management	The analysis and management of risks is an essential part of the security process and shall constitute a continuous and permanently updated activity.	Functional	No Relationship	N/A	N/A	N/A	0	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

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

Focal Document: Spain - Royal Decree 311/2022

Focal Document URL: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-decree-311-2022.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
Article 7(2)	Risk-Based Security Management	Risk management shall enable the maintenance of a controlled environment, minimising risks to acceptable levels. This reduction shall be achieved through the appropriate application of security measures, in a balanced and proportionate manner to the nature of the information processed, the services to be provided and the risks to which they are exposed.	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 with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	10	
Article 8(1)	Prevention, Detection, Response and Conservation	The security of the system shall encompass actions relating to prevention, detection and response, in order to minimise its vulnerabilities and ensure that threats against it are not materialised or, if they are, do not seriously affect the information it handles or the services it provides.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 8(2)	Prevention, Detection, Response and Conservation	Prevention measures, which may incorporate components aimed at deterrence or reducing the exposure surface, shall eliminate or reduce the possibility of threats materialising.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 8(3)	Prevention, Detection, Response and Conservation	Detection measures shall be aimed at discovering the presence of a cyber incident.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
Article 8(4)	Prevention, Detection, Response and Conservation	Response measures, managed in a timely manner, shall be aimed at restoring information and services that may have been affected by a security incident.	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	
Article 8(5)	Prevention, Detection, Response and Conservation	Without prejudice to the other basic principles and minimum requirements, the information system shall guarantee the conservation of data and information in electronic form. The system shall keep services available throughout the entire life cycle of digital information, through a design and procedures that form the basis for the preservation of the digital heritage.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 9(1)	Existence of Lines of Defence	The information system shall have a protection strategy consisting of multiple layers of security, arranged so that when one layer is compromised it allows:	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 9(1)(a)	Existence of Lines of Defence	An adequate reaction to incidents that could not be prevented, reducing the probability of the system being compromised as a whole.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 9(1)(b)	Existence of Lines of Defence	Minimising the final impact on the system.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 9(2)	Existence of Lines of Defence	The lines of defence shall consist of measures of an organisational, physical and logical nature.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 10(1)	Continuous Monitoring and Periodic Reassessment	Continuous monitoring shall enable the detection of anomalous activities or behaviour and a timely response.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 10(2)	Continuous Monitoring and Periodic Reassessment	The permanent evaluation of the security status of assets shall make it possible to measure their evolution, detecting vulnerabilities and identifying configuration deficiencies.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 10(3)	Continuous Monitoring and Periodic Reassessment	Security measures shall be periodically reassessed and updated, adapting their effectiveness to the evolution of risks and protection systems, and potentially leading to a full reassessment of the security posture if necessary.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 11(1)	Differentiation of Responsibilities	In information systems, the information owner, the service owner, the security officer and the system owner shall be distinguished.	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.	8	
Article 11(2)	Differentiation of Responsibilities	Responsibility for the security of information systems shall be distinct from responsibility for the operation of the information systems concerned.	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	
Article 11(2)	Differentiation of Responsibilities	Responsibility for the security of information systems shall be distinct from responsibility for the operation of the information systems concerned.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
Article 11(2)	Differentiation of Responsibilities	Responsibility for the security of information systems shall be distinct from responsibility for the operation of the information systems concerned.	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	
Article 11(3)	Differentiation of Responsibilities	The organisation's security policy shall detail the attributions of each responsible party and the mechanisms for coordination and conflict resolution.	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	
Article 12(1)	Security Policy and Minimum Security Requirements	The information security policy is the set of guidelines governing the way in which an organisation manages and protects the information it processes and the services it provides. To that end, the instrument approving such a security policy shall include, at a minimum, the following:	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	
Article 12(1)(a)	Security Policy and Minimum Security Requirements	The organisation's objectives or mission.	Functional	Intersects With	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
Article 12(1)(b)	Security Policy and Minimum Security Requirements	The regulatory framework within which activities will be carried out.	Functional	Intersects With	Secure Practices Alignment Justification	GOV-01.4	Mechanisms exist to align the organization's Security, Compliance & Resilience Program (SCRP) with one or more industry-recognized frameworks that: (1) Support external scrutiny; and	5	
Article 12(1)(c)	Security Policy and Minimum Security Requirements	Security roles or functions, defining for each their duties and responsibilities, as well as the procedure for their designation and renewal.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 12(1)(d)	Security Policy and Minimum Security Requirements	The structure and composition of the committee or committees for security management and coordination, detailing their area of responsibility and their relationship with other elements of the organisation.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5	
Article 12(1)(e)	Security Policy and Minimum Security Requirements	Guidelines for the structure of the system's security documentation, its management and access.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5	
Article 12(1)(f)	Security Policy and Minimum Security Requirements	The risks arising from the processing of personal data.	Functional	Intersects With	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	5	
Article 12(2)	Security Policy and Minimum Security Requirements	Each public administration shall have a formally approved security policy by the competent body. Likewise, each body or entity with its own legal personality falling within the subjective scope of Article 2 shall have a formally approved security policy by the competent body. However, all or part of the subjects of an institutional public sector may be included within the subjective scope of the security policy approved by the Administration with which they maintain a relationship of linkage, dependence or attachment, where so determined by the competent bodies in the exercise of their organisational powers.	Functional	No Relationship	N/A	N/A	N/A	0	

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

Reference Document: Secure Controls Framework (SCF) version 2026.2

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

Focal Document: Spain - Royal Decree 311/2022

Focal Document URL: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-decree-311-2022.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
Article 12(3)	Security Policy and Minimum Security Requirements	In the General State Administration, each ministry shall have its own security policy, approved by the head of the Department. Public bodies and entities belonging to the state institutional public sector may have their own security policy, approved by the competent body, consistent with that of the Department with which they maintain a relationship of linkage, dependence or attachment, or may fall within the subjective scope of the Department's security policy. Central directorates of the General State Administration that manage services under the declaration of shared services may also have their own security policy, consistent with the Department's policy.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 12(4)	Security Policy and Minimum Security Requirements	The Secretary General of Digital Administration of the Ministry of Economic Affairs and Digital Transformation shall have its own security policy, approved by the head thereof.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 12(5)	Security Policy and Minimum Security Requirements	Municipalities may have a common security policy prepared by the regional or provincial local authority that assumes responsibility for the information security of municipal systems.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 12(6)	Security Policy and Minimum Security Requirements	The security policy shall be established in accordance with the basic principles set out in Chapter II and shall be developed by applying the following minimum requirements:	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
Article 12(6)(a)	Security Policy and Minimum Security Requirements	Organisation and implementation of the security process.	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
Article 12(6)(b)	Security Policy and Minimum Security Requirements	Risk analysis and management.	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 with: (1) The organization's Enterprise Risk Management (ERM); and (2) Industry-recognized cybersecurity risk management practices.	10	
Article 12(6)(c)	Security Policy and Minimum Security Requirements	Personnel management.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
Article 12(6)(d)	Security Policy and Minimum Security Requirements	Professionalism.	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	
Article 12(6)(e)	Security Policy and Minimum Security Requirements	Authorisation and access control.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
Article 12(6)(f)	Security Policy and Minimum Security Requirements	Protection of facilities.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
Article 12(6)(g)	Security Policy and Minimum Security Requirements	Acquisition of security products and contracting of security services.	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	
Article 12(6)(h)	Security Policy and Minimum Security Requirements	Minimum privilege.	Functional	Subset Of	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.	10	
Article 12(6)(i)	Security Policy and Minimum Security Requirements	System integrity and updating.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
Article 12(6)(j)	Security Policy and Minimum Security Requirements	Protection of stored and in-transit information.	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	
Article 12(6)(k)	Security Policy and Minimum Security Requirements	Prevention against other interconnected information systems.	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	
Article 12(6)(l)	Security Policy and Minimum Security Requirements	Activity logging and malicious code detection.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
Article 12(6)(m)	Security Policy and Minimum Security Requirements	Security incidents.	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	
Article 12(6)(n)	Security Policy and Minimum Security Requirements	Continuity of activity.	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	
Article 12(6)(ñ)	Security Policy and Minimum Security Requirements	Continuous improvement of the security process.	Functional	Subset Of	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	10	
Article 12(7)	Security Policy and Minimum Security Requirements	Minimum requirements shall be applied in proportion to the risks identified in each system, in accordance with Article 28, some of which may be omitted in systems with no significant risks.	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	
Article 13(1)	Organisation and Implementation of the Security Process	The security of information systems shall engage all members of the organisation.	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	
Article 13(2)	Organisation and Implementation of the Security Process	The security policy, applying the principle of differentiation of responsibilities referred to in Article 11 and as detailed in section 3.1 of Annex II, shall be known by all persons forming part of the organisation and shall unequivocally identify those responsible for ensuring its compliance, who shall have the following functions:	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
Article 13(2)	Organisation and Implementation of the Security Process	The security policy, applying the principle of differentiation of responsibilities referred to in Article 11 and as detailed in section 3.1 of Annex II, shall be known by all persons forming part of the organisation and shall unequivocally identify those responsible for ensuring its compliance, who shall have the following functions:	Functional	Intersects With	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's security, compliance and resilience policies and provide acknowledgement.	5	
Article 13(2)(a)	Organisation and Implementation of the Security Process	The information owner shall determine the requirements of the information processed.	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 (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	8	
Article 13(2)(a)	Organisation and Implementation of the Security Process	The information owner shall determine the requirements of the information processed.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
Article 13(2)(b)	Organisation and Implementation of the Security Process	The service owner shall determine the requirements of the services provided.	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 (2) Performing a criticality analysis at predefined decision points in the Secure Development Life Cycle (SDLC).	8	
Article 13(2)(b)	Organisation and Implementation of the Security Process	The service owner shall determine the requirements of the services provided.	Functional	Intersects With	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for security, compliance and resilience that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	8	
Article 13(2)(c)	Organisation and Implementation of the Security Process	The security officer shall determine the decisions to satisfy the security requirements of the information and services, shall supervise the implementation of the necessary measures to ensure those requirements are met, and shall report on these matters.	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	

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 - Royal Decree 311/2022

Focal Document URL: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-decree-311-2022.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
Article 13(2)(d)	Organisation and Implementation of the Security Process	The system owner, personally or through own or contracted resources, shall be responsible for developing the specific way of implementing security in the system and supervising its daily operation, and may delegate to administrators or operators under their responsibility.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	8	
Article 13(3)	Organisation and Implementation of the Security Process	The security officer shall be separate from the system owner, with no hierarchical dependency between the two. In exceptional situations where the justified absence of resources makes it necessary for both functions to fall on the same person or on different persons between whom a hierarchical relationship exists, compensatory measures shall be applied to guarantee the purpose of the principle of differentiation of responsibilities provided for in Article 11.	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	
Article 13(3)	Organisation and Implementation of the Security Process	The security officer shall be separate from the system owner, with no hierarchical dependency between the two. In exceptional situations where the justified absence of resources makes it necessary for both functions to fall on the same person or on different persons between whom a hierarchical relationship exists, compensatory measures shall be applied to guarantee the purpose of the principle of differentiation of responsibilities provided for in Article 11.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
Article 13(3)	Organisation and Implementation of the Security Process	The security officer shall be separate from the system owner, with no hierarchical dependency between the two. In exceptional situations where the justified absence of resources makes it necessary for both functions to fall on the same person or on different persons between whom a hierarchical relationship exists, compensatory measures shall be applied to guarantee the purpose of the principle of differentiation of responsibilities provided for in Article 11.	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	
Article 13(4)	Organisation and Implementation of the Security Process	A Security Technical Instruction shall regulate the Certification Scheme for Security Officers, setting out the conditions and requirements applicable to this role.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 13(5)	Organisation and Implementation of the Security Process	In the case of outsourced services, unless for justified and documented reasons, the organisation providing such services shall designate a POC (Point or Person of Contact) for the security of the information processed and the service provided, with the support of the management bodies, to channel and supervise both compliance with the security requirements of the service or solution provided, and communications relating to information security and incident management within the scope of such service. The security POC shall be the Security Officer of the contracted organisation, shall form part of their area or shall have direct communication with it, without prejudice to the ultimate responsibility resting with the public sector entity that is the recipient of said services.	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	
Article 13(5)	Organisation and Implementation of the Security Process	In the case of outsourced services, unless for justified and documented reasons, the organisation providing such services shall designate a POC (Point or Person of Contact) for the security of the information processed and the service provided, with the support of the management bodies, to channel and supervise both compliance with the security requirements of the service or solution provided, and communications relating to information security and incident management within the scope of such service. The security POC shall be the Security Officer of the contracted organisation, shall form part of their area or shall have direct communication with it, without prejudice to the ultimate responsibility resting with the public sector entity that is the recipient of said services.	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	
Article 14(1)	Risk Analysis and Management	Each organisation that develops and implements systems for the processing of information or the provision of services shall carry out its own risk management.	Functional	Intersects With	Security, Compliance & Resilince Outsourcing Limitations	GOV-19.3	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	5	
Article 14(1)	Risk Analysis and Management	Each organisation that develops and implements systems for the processing of information or the provision of services shall carry out its own risk management.	Functional	Intersects With	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security, compliance and resilience controls, compliance and change management.	5	
Article 14(1)	Risk Analysis and Management	Each organisation that develops and implements systems for the processing of information or the provision of services shall carry out its own risk management.	Functional	Intersects With	Outsourcing Non-Essential Functions or Services	SEA-02.2	Mechanisms exist to identify non-essential functions or services that are capable of being outsourced to external service providers and align with the organization's enterprise architecture and security standards.	5	
Article 14(2)	Risk Analysis and Management	This management shall be carried out by means of the analysis and treatment of the risks to which the system is exposed. Without prejudice to the provisions of Annex II, an internationally recognised methodology shall be used.	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	
Article 14(2)	Risk Analysis and Management	This management shall be carried out by means of the analysis and treatment of the risks to which the system is exposed. Without prejudice to the provisions of Annex II, an internationally recognised methodology shall be used.	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	
Article 14(3)	Risk Analysis and Management	The measures adopted to mitigate or eliminate risks shall be justified and, in any case, there shall be proportionality between them and the risks.	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-06.4	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5	
Article 15(1)	Personnel Management	Personnel, whether own or external, related to information systems subject to the provisions of this Royal Decree, shall be trained and informed of their duties, obligations and responsibilities in matters of security. Their actions, which shall be supervised to verify that established procedures are followed, shall apply the approved security norms and operational procedures in the performance of their duties.	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	
Article 15(1)	Personnel Management	Personnel, whether own or external, related to information systems subject to the provisions of this Royal Decree, shall be trained and informed of their duties, obligations and responsibilities in matters of security. Their actions, which shall be supervised to verify that established procedures are followed, shall apply the approved security norms and operational procedures in the performance of their duties.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5	
Article 15(1)	Personnel Management	Personnel, whether own or external, related to information systems subject to the provisions of this Royal Decree, shall be trained and informed of their duties, obligations and responsibilities in matters of security. Their actions, which shall be supervised to verify that established procedures are followed, shall apply the approved security norms and operational procedures in the performance of their duties.	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	
Article 15(2)	Personnel Management	The meaning and scope of the secure use of the system shall be specified and set out in security rules approved by the management or the corresponding superior body.	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	
Article 15(2)	Personnel Management	The meaning and scope of the secure use of the system shall be specified and set out in security rules approved by the management or the corresponding superior body.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5	
Article 16(1)	Professionalism	The security of information systems shall be attended to and reviewed and audited by qualified, dedicated and trained personnel in all phases of their life cycle: planning, design, acquisition, construction, deployment, operation, maintenance, incident management and decommissioning.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	

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 - Royal Decree 311/2022

Focal Document URL: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-decree-311-2022.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
Article 16(1)	Professionalism	The security of information systems shall be attended to and reviewed and audited by qualified, dedicated and trained personnel in all phases of their life cycle: planning, design, acquisition, construction, deployment, operation, maintenance, incident management and decommissioning.	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	
Article 16(2)	Professionalism	The entities within the scope of application of this Royal Decree shall require, in an objective and non-discriminatory manner, that organisations providing security services to them have qualified professionals and appropriate levels of management and maturity in the services provided.	Functional	Intersects With	Security, Compliance & Resilince Outsourcing Limitations	GOV-19.3	Mechanisms exist to ensure organizations involved in developing, implementing and/or maintaining Technology Assets, Applications and/or Services (TAAS) provide assurance of internal oversight capabilities that demonstrate: (1) Governance of internal controls; (2) Risk management, including analysis and mitigation activities; and (3) Compliance with applicable laws, regulations and contractual obligations.	5	
Article 16(2)	Professionalism	The entities within the scope of application of this Royal Decree shall require, in an objective and non-discriminatory manner, that organisations providing security services to them have qualified professionals and appropriate levels of management and maturity in the services provided.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
Article 16(3)	Professionalism	Organisations shall determine the training and experience requirements necessary for personnel to perform their duties.	Functional	Intersects With	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
Article 16(3)	Professionalism	Organisations shall determine the training and experience requirements necessary for personnel to perform their duties.	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	
Article 17	Authorisation and Access Control	Controlled access to information systems within the scope of application of this Royal Decree shall be limited to duly authorised users, processes, devices or other information systems, and exclusively to permitted functions.	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	
Article 18	Protection of Facilities	Information systems and their associated communications infrastructure shall remain in controlled areas and shall have appropriate and proportionate access mechanisms based on the risk analysis, without prejudice to the provisions of Law 8/2011, of April 28, establishing measures for the protection of critical infrastructures and Royal Decree 704/2011, of May 20, approving the Regulation on the protection of critical infrastructures.	Functional	Intersects With	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
Article 19(1)	Acquisition of Security Products and Contracting of Security Services	In the acquisition of security products or contracting of security services for information and communication technologies to be used in information systems within the scope of this Royal Decree, those whose security functionality related to the purpose of acquisition has been certified shall be used, in a manner proportionate to the category of the system and the security level determined.	Functional	Intersects With	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.	5	
Article 19(2)	Acquisition of Security Products and Contracting of Security Services	The Certification Body of the National Scheme for the Evaluation and Certification of Information Technology Security of the National Cryptological Centre (CCN), taking into account nationally and internationally recognised evaluation criteria and methodologies and the intended use of the specific product or service, shall determine the following:	Functional	No Relationship	N/A	N/A	N/A	0	
Article 19(2)(a)	Acquisition of Security Products and Contracting of Security Services	The functional security requirements and certification assurance requirements.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 19(2)(b)	Acquisition of Security Products and Contracting of Security Services	Other additional security certifications required by regulations.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 19(2)(c)	Acquisition of Security Products and Contracting of Security Services	Exceptionally, the criterion to follow in cases where no certified products or services exist.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 19(3)	Acquisition of Security Products and Contracting of Security Services	For the contracting of security services, the provisions of the preceding paragraphs and those of Article 16 shall apply.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 20	Minimum Privilege	Information systems shall be designed and configured granting the minimum privileges necessary for their correct performance, which involves incorporating the following:	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	
Article 20(a)	Minimum Privilege	The system shall provide the essential functionality for the organisation to achieve its competency or contractual objectives.	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	
Article 20(b)	Minimum Privilege	Operation, administration and activity logging functions shall be the minimum necessary, and it shall be ensured that they are only carried out by authorised persons, from likewise authorised locations or equipment; time restrictions and authorised access points may be required if applicable.	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	
Article 20(c)	Minimum Privilege	Functions that are unnecessary or inappropriate to the intended purpose shall be eliminated or deactivated through configuration control. Ordinary use of the system shall be simple and secure, so that insecure use requires a conscious act by the user.	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	
Article 20(c)	Minimum Privilege	Functions that are unnecessary or inappropriate to the intended purpose shall be eliminated or deactivated through configuration control. Ordinary use of the system shall be simple and secure, so that insecure use requires a conscious act by the user.	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	
Article 20(d)	Minimum Privilege	Security configuration guides for different technologies, adapted to the categorisation of the system, shall be applied in order to eliminate or deactivate functions that are unnecessary or inappropriate.	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	
Article 21(1)	System Integrity and Updating	The inclusion of any physical or logical element in the updated inventory of system assets, or its modification, shall require prior formal authorisation.	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	
Article 21(1)	System Integrity and Updating	The inclusion of any physical or logical element in the updated inventory of system assets, or its modification, shall require prior formal authorisation.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.	5	
Article 21(2)	System Integrity and Updating	Permanent evaluation and monitoring shall allow the security status of systems to be adapted by addressing configuration deficiencies, identified vulnerabilities and updates affecting them, as well as the early detection of any incident occurring on them.	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
Article 22(1)	Protection of Information Stored and In Transit	In the organisation and implementation of security, particular attention shall be paid to information stored or in transit through portable or mobile equipment or devices, peripheral devices, information media and communications over open networks, which shall be specifically analysed to achieve adequate protection.	Functional	Intersects With	Use of External Technology Assets, Applications and/or Services (TAAS)	DCH-13	Mechanisms exist to govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.	5	
Article 22(1)	Protection of Information Stored and In Transit	In the organisation and implementation of security, particular attention shall be paid to information stored or in transit through portable or mobile equipment or devices, peripheral devices, information media and communications over open networks, which shall be specifically analysed to achieve adequate protection.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
Article 22(1)	Protection of Information Stored and In Transit	In the organisation and implementation of security, particular attention shall be paid to information stored or in transit through portable or mobile equipment or devices, peripheral devices, information media and communications over open networks, which shall be specifically analysed to achieve adequate protection.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	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 - Royal Decree 311/2022

Focal Document URL: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-esp-decree-311-2022.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
Article 22(2)	Protection of Information Stored and In Transit	Procedures shall be applied to guarantee the recovery and long-term conservation of electronic documents produced by information systems within the scope of this Royal Decree, where this is required.	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	
Article 22(3)	Protection of Information Stored and In Transit	All information on non-electronic media that has been a direct cause or consequence of the electronic information referred to in this Royal Decree shall be protected with the same degree of security as the latter. The measures corresponding to the nature of the medium shall be applied, in accordance with applicable regulations.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
Article 22(3)	Protection of Information Stored and In Transit	All information on non-electronic media that has been a direct cause or consequence of the electronic information referred to in this Royal Decree shall be protected with the same degree of security as the latter. The measures corresponding to the nature of the medium shall be applied, in accordance with applicable regulations.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive and/or regulated data wherever it is processed and/or stored.	5	
Article 23	Prevention Against Other Interconnected Information Systems	The perimeter of the information system shall be protected, particularly when connected to public networks as defined in Law 9/2014, of May 9, General Telecommunications Act, strengthening prevention, detection and response to security incidents. In any case, the risks arising from the interconnection of the system with other systems shall be analysed and their connection point shall be controlled. For the proper interconnection between systems, the provisions of the corresponding Security Technical Instruction shall apply.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
Article 23	Prevention Against Other Interconnected Information Systems	The perimeter of the information system shall be protected, particularly when connected to public networks as defined in Law 9/2014, of May 9, General Telecommunications Act, strengthening prevention, detection and response to security incidents. In any case, the risks arising from the interconnection of the system with other systems shall be analysed and their connection point shall be controlled. For the proper interconnection between systems, the provisions of the corresponding Security Technical Instruction shall apply.	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and; (3) The nature of the information communicated.	3	
Article 24(1)	Activity Logging and Malicious Code Detection	With the purpose of meeting the objective of this Royal Decree, with full guarantees of the right to honour, personal and family privacy and personal image, and in accordance with regulations on personal data protection, civil service or employment law, and other applicable provisions, the activities of users shall be recorded, retaining only strictly necessary information to monitor, analyse, investigate and document undue or unauthorised activities, making it possible to identify the acting person at all times.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
Article 24(2)	Activity Logging and Malicious Code Detection	In order to preserve the security of information systems, and in accordance with the General Data Protection Regulation and its principles of purpose limitation, data minimisation and retention period limitation, entities covered by Article 2 may, to the strictly necessary and proportionate extent, analyse incoming or outgoing communications solely for information security purposes, so as to prevent unauthorised access to networks and information systems, stop denial-of-service attacks, prevent the malicious distribution of harmful code and other damage to said networks and information systems.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
Article 24(3)	Activity Logging and Malicious Code Detection	To correct or, where applicable, enforce accountability, each user accessing the information system shall be uniquely identified so that it is known at all times who has received access rights, what type they are, and who has carried out a particular activity.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
Article 25(1)	Security Incidents	The entity owning the information systems within the scope of this Royal Decree shall have security incident management procedures in accordance with Article 33, the corresponding Security Technical Instruction and, in the case of an essential service operator or digital service provider, in accordance with the annex to Royal Decree 43/2021, of January 26.	Functional	Intersects With	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.	8	
Article 25(2)	Security Incidents	Detection mechanisms, classification criteria, analysis and resolution procedures, as well as channels of communication to interested parties and a record of actions shall also be available. This record shall be used for the continuous improvement of system security.	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	
Article 26	Continuity of Activity	Systems shall have backup copies and the mechanisms necessary to guarantee continuity of operations in the event of loss of usual means shall be established.	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	
Article 27	Continuous Improvement of the Security Process	The integral security process implemented shall be continuously updated and improved. For this purpose, criteria and methods recognised in national and international practice relating to the management of information technology security shall be applied.	Functional	Intersects With	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's Security, Compliance & Resilience Program (SCRP), including: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	5	
Article 28(1)	Compliance with Minimum Requirements	In order to comply with the minimum requirements established in this Royal Decree, entities within its scope of application shall adopt the corresponding security measures and reinforcements indicated in Annex II, taking into account:	Functional	No Relationship	N/A	N/A	N/A	0	
Article 28(1)(a)	Compliance with Minimum Requirements	The assets constituting the information systems concerned.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 28(1)(b)	Compliance with Minimum Requirements	The category of the system, as provided for in Article 40 and Annex I.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 28(1)(c)	Compliance with Minimum Requirements	The decisions adopted to manage the identified risks.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 28(2)	Compliance with Minimum Requirements	The measures referred to in paragraph 1 shall be the minimum required, and may be expanded at the discretion of the security officer, who may include additional measures, taking into account the state of technology, the nature of the information processed or services provided and the risks to which the affected information systems are exposed. The set of selected security measures shall be formalised in a document called the Statement of Applicability, signed by the security officer.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required security, compliance and resilience controls for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5	
Article 28(3)	Compliance with Minimum Requirements	The security measures referenced in Annex II may be replaced by compensatory measures, provided it is documented that they protect, equally or better, against the risk to assets (Annex I) and that the basic principles and minimum requirements in Chapters II and III are satisfied. As an integral part of the Statement of Applicability, the correspondence between compensatory measures implemented and the Annex II measures they compensate shall be indicated in detail. The set shall be subject to formal approval by the security officer.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
Article 29	Common Infrastructure and Services	The use of common infrastructure and services of public administrations, including shared or transversal services, shall facilitate compliance with the provisions of this Royal Decree. The specific cases of use of such infrastructure and services shall be determined by each public administration.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 30(1)	Specific Compliance Profiles and Accreditation of Implementing Entities	By virtue of the principle of proportionality and seeking an effective and efficient application of the ENS to certain entities or specific sectors of activity, specific compliance profiles may be implemented comprising those security measures which, arising from the mandatory risk analysis, are appropriate for a specific security category.	Functional	No Relationship	N/A	N/A	N/A	0	
Article 30(2)	Specific Compliance Profiles and Accreditation of Implementing Entities	In a similar manner, to enable the proper implementation and configuration of solutions or platforms supplied by third parties to be used by entities within the scope of this Royal Decree, accreditation schemes for entities and validation of persons may be implemented to guarantee the security of such solutions or platforms and their compliance with this Royal Decree.	Functional	No Relationship	N/A	N/A	N/A	0	