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

Focal Document: ISO/IEC 27017 (2015)
Focal Document URL: https://www.iso.org/standard/43757.html
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-iso-27017-2015.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1	Scope	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
2	Normative references	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
3	Definitions and abbreviations	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4	Cloud sector-specific concepts	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
4.1	Overview	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	10	
4.2	Supplier relationships in cloud services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
4.3	Relationships between cloud service customers and cloud service providers	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
4.4	Managing information security risks in cloud services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	10	
4.5	Structure of this standard	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5	Information security policies	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	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.	8	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	8	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
5.1	Management direction for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	8	
5.1.1	Policies for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
5.1.1	Policies for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
5.1.1	Policies for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
5.1.1	Policies for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
5.1.1	Policies for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
5.1.2	Review of the policies for information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	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.	10	
6	Organization of information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.1	Internal organization	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.1	Internal organization	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.1	Internal organization	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.1.1	Information security roles and responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
6.1.1	Information security roles and responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
6.1.1	Information security roles and responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	3	
6.1.1	Information security roles and responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
6.1.1	Information security roles and responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
6.1.2	Segregation of duties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.1.2	Segregation of duties	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.1.3	Contact with authorities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	10	
6.1.4	Contact with special interest groups	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the security, compliance and resilience communities to: (1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and (3) Share current cybersecurity and/or data protection-related information including threats, vulnerabilities and incidents.	10	
6.1.5	Information security in project management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.1.5	Information security in project management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Security, Compliance & Resilience In Project Management	PRM-04	Mechanisms exist to assess security, compliance and resilience controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	8	
6.1.5	Information security in project management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	8	

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
6.1.5	Information security in project management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
6.1.5	Information security in project management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.1.5	Information security in project management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
6.1.5	Information security in project management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.1.5	Information security in project management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
6.1.5	Information security in project management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Risk Response	RSK-06.1	remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or	5	
6.1.5	Information security in project management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.2	Mobile devices and teleworking	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
6.2.1	Mobile device policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.2.1	Mobile device policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
6.2.1	Mobile device policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.	5	
6.2.2	Teleworking	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	10	
7	Human resource security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.1	Prior to employment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.1.1	Screening	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	8	
7.1.1	Screening	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
7.1.2	Terms and conditions of employment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	10	
7.1.2	Terms and conditions of employment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
7.1.2	Terms and conditions of employment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	5	
7.1.2	Terms and conditions of employment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	5	
7.1.2	Terms and conditions of employment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
7.2	During employment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	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.	8	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions to this requirement.	8	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Data Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and transparently.	8	
7.2.1	Management responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable data privacy requirements and manage data privacy risks through the organization-wide data privacy program.	8	
7.3	Termination and change of employment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
7.3.1	Termination or change of employment responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.	5	
7.3.1	Termination or change of employment responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
8	Asset management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.1	Responsibility for assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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/regulated data is stored, transmitted or processed.	5	
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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/regulated data flows.	5	
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
8.1.1	Inventory of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
8.1.2	Ownership of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	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.	10	
8.1.3	The acceptable use of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
8.1.3	The acceptable use of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	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.	5	
8.1.3	The acceptable use of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	
8.1.3	The acceptable use of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
8.1.3	The acceptable use of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	8	
8.1.3	The acceptable use of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	
8.1.3	The acceptable use of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
8.1.3	The acceptable use of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Return of Assets	AST-10	Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.	10	
8.1.4	Return of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Return of Assets	AST-10	Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.	10	
8.2	Information classification	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.2.1	Classification of information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.	8	
8.2.1	Classification of information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Asset Scope Classification	AST-04.1	Mechanisms exist to determine security, compliance and resilience control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
8.2.1	Classification of information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
8.2.1	Classification of information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
8.2.2	Labelling of information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	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.	8	
8.2.3	Handling of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
8.2.3	Handling of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	
8.3	Media handling	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
8.3.1	Management of removable media	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
8.3.1	Management of removable media	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	8	
8.3.2	Disposal of media	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	8	
8.3.3	Physical media transfer	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9	Access control	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.1	Business requirements of access control	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.1.1	Access control policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	8	
9.1.2	Access to networks and network services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
9.1.2	Access to networks and network services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.1.2	Access to networks and network services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2	User access management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.2.1	User registration and deregistration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2.1	User registration and deregistration	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2.2	User access provisioning	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2.2	User access provisioning	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2.3	Management of privileged access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2.3	Management of privileged access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2.3	Management of privileged access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2.4	Management of secret authentication information of users	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2.4	Management of secret authentication information of users	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	8	
9.2.4	Management of secret authentication information of users	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	8	
9.2.4	Management of secret authentication information of users	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
9.2.4	Management of secret authentication information of users	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
9.2.4	Management of secret authentication information of users	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
9.2.5	Review of user access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
9.2.5	Review of user access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
9.2.5	Review of user access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
9.2.5	Review of user access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	8	
9.2.5	Review of user access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2.6	Removal or adjustment of access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
9.2.6	Removal or adjustment of access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	8	
9.2.6	Removal or adjustment of access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
9.2.6	Removal or adjustment of access rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	8	
9.3	User responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.3.1	Use of secret authentication information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
9.3.1	Use of secret authentication information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	5	
9.4	System and application access control	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
9.4.1	Information access restriction	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
9.4.1	Information access restriction	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
9.4.1	Information access restriction	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
9.4.1	Information access restriction	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
9.4.2	Secure log-on procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
9.4.2	Secure log-on procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	5	
9.4.2	Secure log-on procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
9.4.2	Secure log-on procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
9.4.2	Secure log-on procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
9.4.3	Password management system	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
9.4.3	Password management system	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
9.4.3	Password management system	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	
9.4.4	Use of privileged utility programs	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	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.	10	
9.4.5	Access control to program source code	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	10	
10	Cryptography	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10.1	Cryptographic controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
10.1.1	Policy on the use of cryptographic controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
10.1.1	Policy on the use of cryptographic controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
10.1.1	Policy on the use of cryptographic controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
10.1.1	Policy on the use of cryptographic controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
10.1.2	Key management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
10.1.2	Key management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
10.1.2	Key management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11	Physical and environmental security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11.1	Secure areas	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11.1.1	Physical security perimeter	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.1.1	Physical security perimeter	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.1.1	Physical security perimeter	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.1.2	Physical entry controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.1.2	Physical entry controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	5	
11.1.2	Physical entry controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.1.3	Securing offices, rooms and facilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	10	
11.1.4	Protecting against external and environmental threats	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
11.1.4	Protecting against external and environmental threats	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
11.1.4	Protecting against external and environmental threats	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
11.1.4	Protecting against external and environmental threats	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
11.1.4	Protecting against external and environmental threats	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
11.1.5	Working in secure areas	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	10	
11.1.6	Delivery and loading areas	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	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.	10	
11.2	Equipment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
11.2.1	Equipment siting and protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	10	
11.2.2	Supporting utilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
11.2.2	Supporting utilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Automatic Voltage Controls	PES-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.	5	
11.2.2	Supporting utilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.2.2	Supporting utilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.2.2	Supporting utilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.2.3	Cabling security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	

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
11.2.3	Cabling security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.2.3	Cabling security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.	8	
11.2.4	Equipment maintenance	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.2.4	Equipment maintenance	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
11.2.4	Equipment maintenance	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
11.2.5	Removal of assets	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Removal of Assets	AST-11	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	10	
11.2.6	Security of equipment and assets off-premises	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.2.6	Security of equipment and assets off-premises	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	5	
11.2.6	Security of equipment and assets off-premises	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.2.6	Security of equipment and assets off-premises	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
11.2.6	Security of equipment and assets off-premises	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Logical Tampering Protection	AST-15	Mechanisms exist to assess the integrity of critical Technology Assets, Applications and/or Services (TAAS) to detect evidence of tampering, where: (1) Logical assessments evaluate the integrity of critical components (e.g., configuration settings); and (2) Physical assessments evaluate assets for evidence of unauthorized access and/or modifications.	5	
11.2.6	Security of equipment and assets off-premises	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
11.2.7	Secure disposal or reuse of equipment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
11.2.8	Unattended user equipment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended technology assets to protect against tampering and unauthorized access.	10	
11.2.9	Clear desk and clear screen policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
11.2.9	Clear desk and clear screen policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	5	
11.2.9	Clear desk and clear screen policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
12	Operations security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12.1	Operational procedures and responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12.1.1	Documented operating procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Security, Compliance & Resilience Program (SCRP)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	5	
12.1.1	Documented operating procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
12.1.1	Documented operating procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
12.1.1	Documented operating procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5	
12.1.1	Documented operating procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8	
12.1.1	Documented operating procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
12.1.2	Change management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
12.1.2	Change management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
12.1.2	Change management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
12.1.2	Change management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
12.1.2	Change management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
12.1.3	Capacity management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
12.1.3	Capacity management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
12.1.4	Separation of development, testing and operational environments	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
12.1.4	Separation of development, testing and operational environments	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
12.2	Protection from malware	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12.2.1	Controls against malware	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	8	
12.2.1	Controls against malware	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	8	
12.3	Backup	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12.3.1	Information backup	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
12.3.1	Information backup	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
12.3.1	Information backup	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
12.3.1	Information backup	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	8	
12.4	Logging and monitoring	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12.4.1	Event logging	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
12.4.1	Event logging	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
12.4.1	Event logging	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
12.4.1	Event logging	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
12.4.1	Event logging	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	8	
12.4.1	Event logging	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
12.4.1	Event logging	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
12.4.1	Event logging	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
12.4.2	Protection of log information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	
12.4.3	Administrator and operator logs	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	10	
12.4.4	Clock synchronization	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	10	
12.5	Control of operational software	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12.5.1	Installation of software on operational systems	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
12.5.1	Installation of software on operational systems	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to Technology Assets, Applications and/or Services (TAAS).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
12.6	Technical vulnerability management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12.6.1	Management of technical vulnerabilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
12.6.1	Management of technical vulnerabilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
12.6.1	Management of technical vulnerabilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
12.6.1	Management of technical vulnerabilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
12.6.2	Restrictions on software installation	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	10	
12.7	Information systems audit considerations	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
12.7.1	Information systems audit controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
12.7.1	Information systems audit controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
12.7.1	Information systems audit controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Audit Activities	CPL-04	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	5	
13	Communications security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
13.1	Network security management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
13.1.1	Network controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.1.1	Network controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
13.1.1	Network controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	8	
13.1.1	Network controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
13.1.1	Network controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
13.1.1	Network controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	
13.1.1	Network controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.1.2	Security of network services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.1.2	Security of network services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	8	
13.1.2	Security of network services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.1.2	Security of network services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	8	
13.1.2	Security of network services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.1.2	Security of network services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.1.3	Segregation in networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	8	
13.1.3	Segregation in networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.1.3	Segregation in networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2	Information transfer	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	5	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	8	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.1	Information transfer policies and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
13.2.2	Agreements on information transfer	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.2	Agreements on information transfer	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.2	Agreements on information transfer	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
13.2.3	Electronic messaging	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
13.2.3	Electronic messaging	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	8	
13.2.4	Confidentiality or non-disclosure agreements	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
13.2.4	Confidentiality or non-disclosure agreements	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
14	System acquisition, development and maintenance	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
14.1	Security requirements of information systems	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
14.1.1	Information security requirements analysis and specification	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
14.1.1	Information security requirements analysis and specification	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Security, Compliance & Resilience Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
14.1.1	Information security requirements analysis and specification	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
14.1.2	Securing applications services on public networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
14.1.2	Securing applications services on public networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
14.1.2	Securing applications services on public networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
14.1.3	Protecting application services transactions	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
14.1.3	Protecting application services transactions	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
14.2	Security in development and support processes	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
14.2.1	Secure development policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
14.2.1	Secure development policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
14.2.2	System change control procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	10	
14.2.2	System change control procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
14.2.3	Technical review of applications after operating platform changes	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
14.2.4	Restrictions on changes to software packages	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
14.2.4	Restrictions on changes to software packages	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	8	
14.2.5	Secure system engineering principles	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
14.2.5	Secure system engineering principles	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
14.2.6	Secure development environment	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	10	
14.2.7	Outsourced development	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
14.2.7	Outsourced development	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	3	
14.2.7	Outsourced development	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
14.2.8	System security testing	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
14.2.8	System security testing	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
14.2.9	System acceptance testing	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
14.2.9	System acceptance testing	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
14.2.9	System acceptance testing	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
14.3	Test data	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
14.3.1	Protection of test data	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	8	
15	Supplier relationships	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
15.1	Information security in supplier relationships	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
15.1.1	Information security policy for supplier relationships	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
15.1.1	Information security policy for supplier relationships	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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).	8	
15.1.2	Addressing security within supplier agreements	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	10	
15.1.3	Information and communication technology supply chain	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	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.	10	
15.2	Supplier service delivery management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
15.2.1	Monitoring and review of supplier services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	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.	10	
15.2.2	Managing changes to supplier services	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	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.	10	
16	Information security incident management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
16.1	Management of information security incidents and improvements	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
16.1.1	Responsibilities and procedures	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
16.1.2	Reporting information security events	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8	
16.1.3	Reporting information security weaknesses	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
16.1.4	Assessment of and decision on information security events	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
16.1.4	Assessment of and decision on information security events	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
16.1.5	Response to information security incidents	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
16.1.5	Response to information security incidents	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
16.1.6	Learning from information security incidents	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	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.	10	
16.1.7	Collection of evidence	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	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.	10	
17	Information security aspects of business continuity management	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
17.1	Information security continuity	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
17.1.1	Planning information security continuity	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	

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
17.1.2	Implementing information security continuity	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
17.1.3	Verify, review and evaluate information security continuity	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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.	8	
17.2	Redundancies	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
17.2.1	Availability of information processing facilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
17.2.1	Availability of information processing facilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
17.2.1	Availability of information processing facilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
18	Compliance	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
18.1	Compliance with legal and contractual requirements	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
18.1.1	Identification of applicable legislation and contractual requirements	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
18.1.2	Intellectual property rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5	
18.1.3	Protection of records	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	8	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Reasonable Data Privacy Practices	PRI-01.11	Mechanisms exist to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.	8	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Choice & Consent	PRI-03	Mechanisms exist to enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with: (1) Plain language to illustrate the potential data privacy risks of the authorization; (2) A means for users to decline the authorization; and (3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.	5	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.	5	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Internal Use of Personal Data (PD) For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: (1) Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and (2) Authorizes the use of PD when such information is required for internal testing, training and research.	5	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, sharing and/or updating Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the data privacy notice and with the implicit or explicit consent of the data subject.	5	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
18.1.4	Privacy and protection of personally identifiable information	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
18.1.5	Regulation of cryptographic controls	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Subset Of	Export-Controlled Cryptography	CRY-01.2	Mechanisms exist to address the exporting of cryptographic technologies in compliance with relevant statutory and regulatory requirements.	10	
18.2	Information security reviews	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
18.2.1	Independent review of information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	5	
18.2.1	Independent review of information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
18.2.1	Independent review of information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	5	
18.2.1	Independent review of information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
18.2.1	Independent review of information security	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Audit Activities	CPL-04	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	5	
18.2.2	Compliance with security policies and standards	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	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	
18.2.2	Compliance with security policies and standards	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Security, Compliance & Resilience Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's security, compliance and/or resilience policies, standards and other applicable requirements.	5	
18.2.2	Compliance with security policies and standards	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
18.2.2	Compliance with security policies and standards	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Personal Data (PD) Control Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct testing, training and monitoring activities for Personal Data (PD) controls.	5	
18.2.3	Technical compliance review	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	3	
18.2.3	Technical compliance review	For specific requirement details, buy a licensed copy of the Focal Document at: https://www.iso.org/standard/43757.html	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	8	