

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:
Published Document URL:

IEC 62443-2-1 (2024)
<https://webstore.iec.ch/en/publication/62883>
<https://content.securecontrolsframework.com/strm/scf-strm-general-iec-62443-2-1-2024.pdf>

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
ORG 1.1	Information security management system (ISMS)	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Security, Compliance & Resilience Program (SCRp)	GOV-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience governance controls.	10	
ORG 1.2	Background checks	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Equal	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
ORG 1.3	Security roles and responsibilities	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
ORG 1.4	Security awareness training	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	8	
ORG 1.4	Security awareness training	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8	
ORG 1.5	Security responsibilities training	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
ORG 1.6	Supply chain security	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
ORG 2.1	Security risk mitigation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	8	
ORG 2.1	Security risk mitigation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
ORG 2.1	Security risk mitigation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	8	
ORG 2.1	Security risk mitigation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
ORG 2.2	Processes for discovery of security anomalies	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
ORG 2.2(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	8	
ORG 2.2(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	8	
ORG 2.2(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Unauthorized Network Services	MON-11.2	Automated mechanisms exist to detect unauthorized network services and alert incident response personnel.	8	
ORG 2.2(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	8	
ORG 2.2(d)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
ORG 2.3	Secure development and support	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
ORG 2.3	Secure development and support	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	8	
ORG 2.4	SP reviews	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
ORG 2.4(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
ORG 2.4(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	8	
ORG 2.4(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Threat Analysis & Flow Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	8	
ORG 2.4(d)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	8	
ORG 3.1	Physical access control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Physical & Environmental Protections	PE-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
CM 1.1	Asset inventory baseline	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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.	10	
CM 1.1(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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.	10	
CM 1.1(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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.	10	
CM 1.1(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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.	10	
CM 1.1(d)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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.	10	
CM 1.1(e)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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.	10	
CM 1.1(f)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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.	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
CM 1.1(g)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAAS) that: (1) Accurately reflects the current TAAS 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.	10	
CM 1.1(h)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAAS) that: (1) Accurately reflects the current TAAS 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.	10	
CM 1.1(i)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAAS) that: (1) Accurately reflects the current TAAS 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.	10	
CM 1.2	Infrastructure drawings/documentation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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/regulatory data flows.	10	
CM 1.3	Configuration settings	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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.	8	
CM 1.3	Configuration settings	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	8	
CM 1.4	Change control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
CM 1.4	Change control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	8	
NET 1.1	Segmentation from non-IACS zones	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Network Segmentation (macrosegmentation)	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.	10	
NET 1.2	Documentation of zones and network zone interconnections	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
NET 1.2	Documentation of zones and network zone interconnections	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
NET 1.2	Documentation of zones and network zone interconnections	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Interconnection Security Agreements (ISAs)	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs), or similar methods, that document, for each interconnection: (1) Interface characteristics; (2) Security, compliance and resilience requirements; and (3) The nature of the information communicated.	3	
NET 1.3	Network segmentation from safety systems	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
NET 1.3	Network segmentation from safety systems	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	5	
NET 1.3	Network segmentation from safety systems	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.	5	
NET 1.3	Network segmentation from safety systems	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Network Segmentation (macrosegmentation)	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.	5	
NET 1.4	Network autonomy	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Fail Safe	SEA-07.3	Mechanisms exist to implement fail-safe procedures when failure conditions occur.	5	
NET 1.5	Network disconnection from external networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive/regulatory data enclaves (secure zones).	3	
NET 1.6	Internal network access control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Data Flow Enforcement - Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5	
NET 1.6	Internal network access control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	5	
NET 1.7	Network accessible services	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Isolation of System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate Technology Assets, Applications and/or Services (TAAS) that support critical missions and/or business functions.	3	
NET 1.7	Network accessible services	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
NET 1.8	User messaging	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
NET 1.8	User messaging	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	End-User Messaging Technologies	NET-12.2	Mechanisms exist to prohibit the transmission of unprotected sensitive/regulatory data by end-user messaging technologies.	5	
NET 1.9	Network time distribution	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	10	
NET 2.1	Wireless protocols	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	10	
NET 2.1(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
NET 2.1(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.	5	
NET 2.1(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
NET 2.2	Wireless network segmentation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Network Segmentation (macrosegmentation)	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.	10	
NET 2.3	Wireless properties and addresses	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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.	8	
NET 3.1	Remote access applications	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	10	
NET 3.2	Remote access connections	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	10	
NET 3.2(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3	
NET 3.2(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3	
NET 3.2(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3	
NET 3.2(d)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3	
NET 3.2(e)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3	
NET 3.2(f)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3	
NET 3.2(g)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3	
NET 3.2(h)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3	
NET 3.3	Remote access termination	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	5	
NET 3.3	Remote access termination	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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.	8	
COMP 1.1	Component hardening	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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.	10	
COMP 1.2	Dedicated portable media	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	8	
COMP 1.2	Dedicated portable media	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	8	
COMP 2.1	Malware free	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	8	
COMP 2.1	Malware free	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	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
COMP 2.2	Malware protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimicrobial technologies to detect and eradicate malicious code.	10	
COMP 2.3	Malware protection software validation and installation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimicrobial technologies, including signature definitions.	5	
COMP 2.3	Malware protection software validation and installation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Malware Protection Mechanism Testing	END-04.5	Mechanisms exist to test antimicrobial technologies by introducing a known benign, non-spreading test case into the system and subsequently verifying that both detection of the test case and associated incident reporting occurs.	5	
COMP 3.1	Security patch authenticity/integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Software Patch Integrity	VPM-05.8	Mechanisms exist to ensure software and/or firmware patches are: (1) Obtained from trusted sources; and (2) Checked for integrity.	8	
COMP 3.2	Security patch validation and installation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Pre-Deployment Patch Testing	VPM-05.6	Mechanisms exist to perform due diligence on software and/or firmware update stability by conducting pre-production testing in a non-production environment.	8	
COMP 3.3	Security patch status	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	8	
COMP 3.4	Security patching retention of security	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a production environment before changes are implemented in a production environment.	8	
COMP 3.4	Security patching retention of security	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Pre-Deployment Patch Testing	VPM-05.6	Mechanisms exist to perform due diligence on software and/or firmware update stability by conducting pre-production testing in a non-production environment.	5	
COMP 3.5	Security patch mitigation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
COMP 3.5	Security patch mitigation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Deferred Patching Decisions	VPM-04.3	Mechanisms exist to facilitate the deferral of software and/or firmware patches when the disadvantages of applying the patch outweighs the benefits.	8	
DATA 1.1	Data classification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	10	
DATA 1.2	Data confidentiality	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
DATA 1.2	Data confidentiality	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	8	
DATA 1.2	Data confidentiality	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
DATA 1.3	Safety system configuration mode	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Safety Assessment	EMB-15	Mechanisms exist to evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure.	3	
DATA 1.3(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	3	
DATA 1.3(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	3	
DATA 1.4	Data retention policy	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
DATA 1.5	Cryptographic mechanisms	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
DATA 1.6	Key management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	10	
DATA 1.7	Data Integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	8	
DATA 1.7	Data Integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical Technology Assets, Applications and/or Services (TAAS) to generate alerts for unauthorized modifications.	5	
USER 1.1	User identity assignment	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Identity & Access Management (IAM)	IAI-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
USER 1.1	User identity assignment	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Identification & Authentication for Organizational Users	IAI-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	8	
USER 1.1	User identity assignment	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAI-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	8	
USER 1.1	User identity assignment	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Identification & Authentication for Devices	IAI-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	8	
USER 1.1	User identity assignment	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAI-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	8	
USER 1.2	User identity removal	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	User Provisioning & De-Provisioning	IAI-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	8	
USER 1.2	User identity removal	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Account Management	IAI-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	8	
USER 1.3	User identity persistence	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Account Management	IAI-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	8	
USER 1.3	User identity persistence	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automated System Account Management (Directory Services)	IAI-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
USER 1.4	Access rights assignment	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAI-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
USER 1.4	Access rights assignment	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automated System Account Management (Directory Services)	IAI-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	8	
USER 1.5	Least privilege	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Role-Based Access Control (RBAC)	IAI-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.	10	
USER 1.6	Software service authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAI-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	8	
USER 1.6	Software service authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAI-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	8	
USER 1.7	Software services interactive login rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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.	8	
USER 1.7	Software services interactive login rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAI-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
USER 1.7	Software services interactive login rights	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automated System Account Management (Directory Services)	IAI-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
USER 1.8	Human user authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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.	8	
USER 1.8	Human user authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automated System Account Management (Directory Services)	IAI-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
USER 1.8(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automated System Account Management (Directory Services)	IAI-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
USER 1.8(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automated System Account Management (Directory Services)	IAI-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
USER 1.8(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Automated System Account Management (Directory Services)	IAI-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
USER 1.9	Multifactor authentication (MFA)	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Multi-Factor Authentication (MFA)	IAI-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	10	
USER 1.10	Mutual authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Mutual Authentication (MA)	IAI-30	Mechanisms exist to enforce Mutual Authentication (MA) where both sides of a communications channel verify the identity of the other party through certificate exchange.	10	
USER 1.11	Password protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Authenticator Management	IAI-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.	10	
USER 1.11	Password protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Password-Based Authentication	IAI-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	8	
USER 1.12	Shared and disclosed/compromised passwords	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Events Requiring Authenticator Change	IAI-10.13	Mechanisms exist to change authentication credentials: (1) At predefined intervals; and/or (2) Upon suspicion of credential compromise.	8	
USER 1.12	Shared and disclosed/compromised passwords	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAI-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	8	
USER 1.13	User login display information	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Equal	Previous Logon Notification	SEA-19	Mechanisms exist to configure systems that process, store or transmit sensitive/regulated data to notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.	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
USER 1.14	User login failure displays	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	5	
USER 1.15	Consecutive login failures	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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.	8	
USER 1.16	Session integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Equal	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	10	
USER 1.17	Concurrent sessions	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Equal	Concurrent Session Control	IAC-23	Mechanisms exist to limit the number of concurrent sessions for each system account.	10	
USER 1.18	Screen lock	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Equal	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	10	
USER 1.19	Component authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	8	
USER 2.1	Authorization	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	10	
USER 2.2	Separation of duties	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Equal	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	10	
USER 2.3	Multiple approvals	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical Technology Assets, Applications and/or Services (TAAS).	8	
USER 2.3	Multiple approvals	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Dual Authorization for Privileged Commands	IAC-20.5	Automated mechanisms exist to enforce dual authorization for privileged commands.	8	
USER 2.4	Manual elevation of privileges	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Dual Authorization for Privileged Commands	IAC-20.5	Automated mechanisms exist to enforce dual authorization for privileged commands.	8	
EVENT 1.1	Event detection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Event Log Analysis & Triage	MON-17	Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response procedures.	10	
EVENT 1.2	Event reporting	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	10	
EVENT 1.3	Event reporting interfaces	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
EVENT 1.4	Logging	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
EVENT 1.4	Logging	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	8	
EVENT 1.5	Log entries	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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.	10	
EVENT 1.6	Log access	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
EVENT 1.7	Event analysis	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	10	
EVENT 1.8	Incident handling and response	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
EVENT 1.8	Incident handling and response	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
EVENT 1.9	Vulnerability handling	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
AVAIL 1.1	Continuity management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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 (BCDR) playbooks).	10	
AVAIL 1.2	Resource availability management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	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	
AVAIL 1.3	Failure-state	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Restore Within Time Period	BCD-12.4	Mechanisms exist to restore Technology Assets, Applications, Services and/or Data (TAASD) within organization-defined restoration time-periods from configuration-controlled and integrity-protected information, representing a known, operational state for the asset.	8	
AVAIL 1.3	Failure-state	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	8	
AVAIL 2.1	Backup	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Subset Of	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).	10	
AVAIL 2.2	Backup non-interference	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
AVAIL 2.3	Backup verification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	8	
AVAIL 2.4	Backup media	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	
AVAIL 2.4	Backup media	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
AVAIL 2.5	Backup restoration	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/62883	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	8	