

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

Reference document: Secure Controls Framework (SCF) version 2026.1
 STRM Guidance: <https://securecontrolsframework.com/start-hereset-theory-relationship-mapping-strm/>

Focal Document:
 Focal Document URL:
 Published STRM URL:

IEC 62443-3-3 (2013)
<https://webstore.iec.ch/en/publication/7033>
<https://content.securecontrolsframework.com/strm/scf-strm-general-iec-62443-3-3-2013.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
SR 1.1	Human user identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 1.1	Human user identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAc-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	8	
SR 1.1 RE 1	Unique identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAc-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	
SR 1.1 RE 1	Unique identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 1.1 RE 1	Unique identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAc-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	8	
SR 1.1 RE 2	Multi-factor authentication for untrusted networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAc-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/regulared data.	8	
SR 1.2	Software process and device identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Identification & Authentication for Devices	IAc-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	5	
SR 1.2	Software process and device identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAc-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	5	
SR 1.2 RE 1	Unique identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Identification & Authentication for Devices	IAc-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically-based and replay resistant.	5	
SR 1.2 RE 1	Unique identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAc-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	5	
SR 1.3	Account management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Account Management	IAc-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	
SR 1.3	Account management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Automated System Account Management (Directory Services)	IAc-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	8	
SR 1.3 RE 1	Unified account management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Automated System Account Management (Directory Services)	IAc-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
SR 1.4	Identifier management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Identifier Management (User Names)	IAc-09	Mechanisms exist to govern naming standards for usernames and Technology Assets, Applications and/or Services (TAAS).	10	
SR 1.4	Identifier management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	User Identity (ID) Management	IAc-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	0	No applicable SCF control
SR 1.5	Authenticator management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SR 1.5(h)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAc-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	Lettering started at (h)
SR 1.5(i)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAc-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	Lettering started at (h)
SR 1.5(j)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAc-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	Lettering started at (h)
SR 1.5(k)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAc-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	Lettering started at (h)
SR 1.5 RE 1	Hardware security for software process identity credentials	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Hardware Security Modules (HSM)	IAc-12.1	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	10	
SR 1.6	Wireless access management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect the confidentiality and integrity of wireless networking technologies by implementing authentication and strong encryption.	10	
SR 1.6 RE 1	Unique identification and authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
SR 1.7	Strength of password-based authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 1.7 RE 1	Password generation and lifetime restrictions for human users	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 1.7 RE 2	Password lifetime restrictions for all users	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 1.8	Public key infrastructure (PKI) certificates	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	PKI-Based Authentication	IAc-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
SR 1.9	Strength of public key authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SR 1.9(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	PKI-Based Authentication	IAc-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
SR 1.9(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	PKI-Based Authentication	IAc-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
SR 1.9(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	PKI-Based Authentication	IAc-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
SR 1.9(d)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	PKI-Based Authentication	IAc-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
SR 1.9(e)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	PKI-Based Authentication	IAc-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.	10	
SR 1.9 RE 1	Hardware security for public key authentication	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Hardware Security Modules (HSM)	IAc-12.1	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.	10	
SR 1.10	Authenticator feedback	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Equal	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.	10	
SR 1.11	Unsuccessful login attempts	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 1.12	System use notification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS).	10	
SR 1.12	System use notification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Standardized Microsoft Windows Banner	SEA-18.1	Mechanisms exist to configure Microsoft Windows-based systems to display an approved logon banner before granting access to the system.	8	
SR 1.12	System use notification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Truncated Banner	SEA-18.2	Mechanisms exist to utilize a truncated system use notification / logon banner on systems not capable of displaying a logon banner from a centralized directory services technology (e.g., Active Directory), Entra ID.	8	
SR 1.13	Access via untrusted networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	DMZ Networks	NET-08.1	Mechanisms exist to monitor DMZ-Mitigated Zone (DMZ) network segments to separate untrusted networks from trusted networks.	5	
SR 1.13 RE 1	Explicit access request approval	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 2.1	Authorization enforcement	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 2.1 RE 1	Authorization enforcement for all users	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 2.1 RE 2	Permission mapping to roles	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	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.	10	
SR 2.1 RE 3	Supervisor override	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Equal	Manual Override	IAc-16.5	Mechanisms exist to enable a manual override of the current account privileges to enable the timely response to unusual conditions without terminating the current session and establishing a new session as a higher-privileged user.	10	
SR 2.1 RE 4	Dual approval	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Dual Authorization for Privileged Commands	IAc-20.5	Automated mechanisms exist to enforce dual authorization for privileged commands.	10	
SR 2.2	Wireless use control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 2.2	Wireless use control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	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
SR 2.2 RE 1	Identify and report unauthorized wireless devices	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Wireless Network Monitoring	MON-01.5	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and (2) Anomalous and/or hostile activities.	10	
SR 2.3	Use control for portable and mobile devices	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
SR 2.3(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Restricting Access To Authorized Technology Assets, Applications and/or Services (TAAS)	MDM-11	Mechanisms exist to restrict the connectivity of unauthorized mobile devices from communicating with organizational Technology Assets, Applications and/or Services (TAAS).	8	
SR 2.3(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	8	
SR 2.3(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Restricting Access To Authorized Technology Assets, Applications and/or Services (TAAS)	MDM-11	Mechanisms exist to restrict the connectivity of unauthorized mobile devices from communicating with organizational Technology Assets, Applications and/or Services (TAAS).	8	
SR 2.3 RE 1	Enforcement of security status of portable and mobile devices	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Restricting Access To Authorized Technology Assets, Applications and/or Services (TAAS)	MDM-11	Mechanisms exist to restrict the connectivity of unauthorized mobile devices from communicating with organizational Technology Assets, Applications and/or Services (TAAS).	8	
SR 2.4	Mobile code	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	8	
SR 2.4(a)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	8	
SR 2.4(b)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	8	
SR 2.4(c)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	8	
SR 2.4(d)	N/A	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	8	
SR 2.4 RE 1	Mobile code integrity check	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	5	
SR 2.5	Session lock	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 2.6	Remote session termination	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Equal	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	10	
SR 2.7	Concurrent session control	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Equal	Concurrent Session Control	IAC-23	Mechanisms exist to limit the number of concurrent sessions for each system account.	10	
SR 2.8	Auditable events	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	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.	10	
SR 2.8 RE 1	Centrally managed, system-wide audit trail	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 2.8 RE 1	Centrally managed, system-wide audit trail	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	8	
SR 2.9	Audit storage capacity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	10	
SR 2.9 RE 1	Warn when audit record storage capacity threshold reached	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Event Log Storage Capacity Alerting	MON-05.2	Automated mechanisms exist to alert appropriate personnel when the allocated volume reaches an organization-defined percentage of maximum event log storage capacity.	10	
SR 2.10	Response to audit processing failures	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Response To Event Log Processing Failures	MON-05	Mechanisms exist to alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption.	10	
SR 2.11	Timestamps	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Time Stamps	MON-07	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs.	10	
SR 2.11 RE 1	Internal time synchronization	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	10	
SR 2.12	Non-repudiation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Non-Repudiation	MON-09	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.	10	
SR 2.12 RE 1	Non-repudiation for all users	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Non-Repudiation	MON-09	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.	10	
SR 3.1	Communication integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	10	
SR 3.1 RE 1	Cryptographic integrity protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Equal	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	10	
SR 3.2	Malicious code protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	10	
SR 3.2 RE 1	Malicious code protection on entry and exit points	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize anti-malware technologies to detect and eradicate malicious code.	8	
SR 3.2 RE 2	Central management and reporting for malicious code protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage anti-malware technologies.	10	
SR 3.3	Security functionality verification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 3.3	Security functionality verification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Control Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security, compliance and resilience controls following implemented changes to ensure applicable controls operate as designed.	8	
SR 3.3 RE 1	Automated mechanisms for security functionality verification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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.	3	
SR 3.3 RE 2	Security functionality verification during normal operation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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.	3	
SR 3.4	Software and information integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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.	8	
SR 3.4 RE 1	Automated notification about integrity violations	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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.	8	
SR 3.5	Input validation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.	10	
SR 3.6	Deterministic output	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	No Relationship	N/A	N/A	N/A	0	No applicable SCF control
SR 3.7	Error handling	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Error Handling	TDA-19	Mechanisms exist to handle error conditions by: (1) Identifying potentially security-relevant error conditions; (2) Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and (3) Revealing error messages only to authorized personnel.	5	
SR 3.8	Session integrity	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	10	
SR 3.8 RE 1	Invalidation of session ID after session termination	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Invalidate Session Identifiers at Logout	NET-09.1	Automated mechanisms exist to invalidate session identifiers upon user logout or other session termination.	10	
SR 3.8 RE 2	Unique session ID generation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Unique System-Generated Session Identifiers	NET-09.2	Automated mechanisms exist to generate and recognize unique session identifiers for each session.	10	
SR 3.8 RE 3	Randomness of session IDs	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Unique System-Generated Session Identifiers	NET-09.2	Automated mechanisms exist to generate and recognize unique session identifiers for each session.	5	
SR 3.9	Protection of audit information	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 3.9 RE 1	Audit records on write-once media	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Write Once Read Many (WORM) Event Log Generation	MON-19	Mechanisms exist to produce event logs on hardware-enforced, write-once media (e.g., Write Once Read Many (WORM) technologies).	5	
SR 4.1	Information confidentiality	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 4.1 RE 1	Protection of confidentiality at rest or in transit via untrusted networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 4.1 RE 2	Protection of confidentiality across zone boundaries	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
SR 4.2	Information persistence	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Non-Persistence	SEA-08	Mechanisms exist to implement non-persistent system components and services that are initiated in a known state and terminated upon the end of the session of use or periodically at an organization-defined frequency.	5	
SR 4.2 RE 1	Purging of shared memory resources	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Non-Persistence	SEA-08	Mechanisms exist to implement non-persistent system components and services that are initiated in a known state and terminated upon the end of the session of use or periodically at an organization-defined frequency.	5	
SR 4.3	Use of cryptography	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 5.1	Network segmentation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 5.1 RE 1	Physical network segmentation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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.	3	
SR 5.1 RE 2	Independence from non-control system networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.	8	

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
SR 5.1 RE 3	Logical and physical isolation of critical networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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/regulated data enclaves (secure zones).	8	
SR 5.2	Zone boundary protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 5.2 RE 1	Deny by default, allow by exception	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Equal	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).	10	
SR 5.2 RE 2	Island mode	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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/regulated data enclaves (secure zones).	3	
SR 5.2 RE 3	Fail close	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Fail Secure	SEA-07.2	Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure.	3	
SR 5.3	General purpose person-to-person communication restrictions	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 5.3 RE 1	Prohibit all general purpose person-to-person communications	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 5.4	Application partitioning	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	10	
SR 6.1	Audit log accessibility	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Access by Subset of Privileged Users	MON-08.2	Mechanisms exist to restrict access to the management of event logs to privileged users with a specific business need.	10	
SR 6.1 RE 1	Programmatic access to audit logs	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	8	
SR 6.2	Continuous monitoring	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
SR 7.1	Denial of service protection	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	10	
SR 7.1 RE 1	Manage communication loads	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	8	
SR 7.1 RE 2	Limit DoS effects to other systems or networks	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Intersects With	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	8	
SR 7.2	Resource management	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 7.3	Control system backup	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 7.3 RE 1	Backup verification	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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.	5	
SR 7.3 RE 2	Backup automation	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 7.4	Control system recovery and reconstitution	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 7.5	Emergency power	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Subset Of	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.	10	
SR 7.6	Network and security configuration settings	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 7.6	Network and security configuration settings	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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).	8	
SR 7.6 RE 1	Machine-readable reporting of current security settings	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	
SR 7.7	Least functionality	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	Functional	Equal	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.	10	
SR 7.8	Control system component inventory	For specific requirement details, buy a licensed copy of the Focal Document at: https://webstore.iec.ch/en/publication/7033	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	