Set Theory Relationship Mapping (STRM)

Reference Document : **Secure Controls Framework (SCF) version 2024.4**

Focal Document: **NIST SP 800-171A**

Focal Document URL: **https://csrc.nist.gov/pubs/sp/800/171/a/final**

STRM URL: **https://securecontrolsframework.com/content/strm/scf-strm-nist-800-171a.pdf**

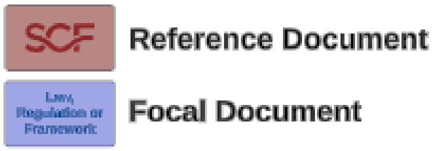
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

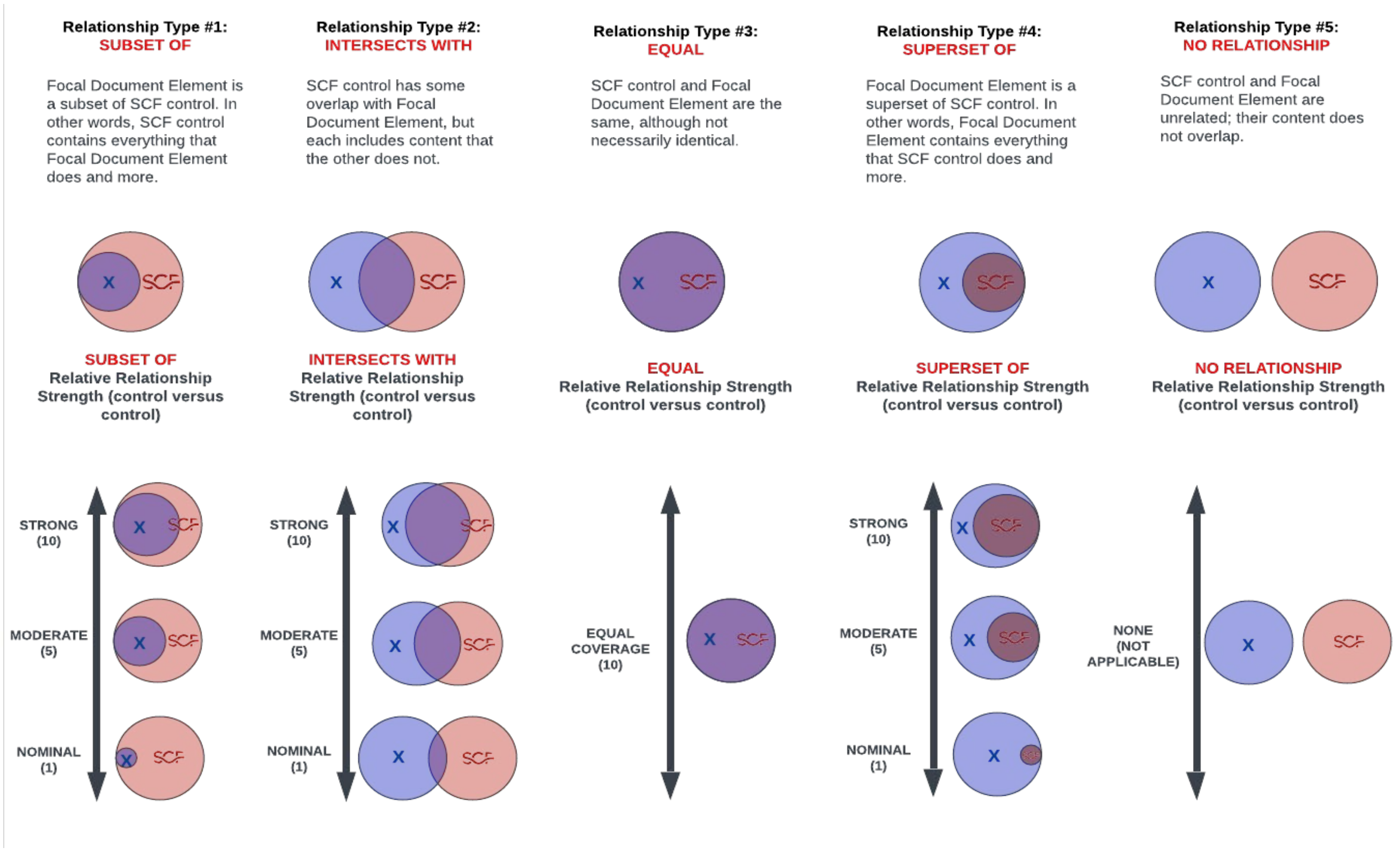
STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

1. **Syntactic**: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
2. **Semantic**: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
3. **Functional**: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

1. **Subset Of**
2. **Intersects With**
3. **Equal**
4. **Superset Of**
5. **No Relationship**





Relationship Type #1: **SUBSET OF**

Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

Relationship Type #2: **INTERSECTS WITH**

SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

Relationship Type #3: **EQUAL**

SCF control and Focal Document Element are the same, although not necessarily identical.

Relationship Type #4: **SUPERSET OF**

Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

Relationship Type #5: **NO RELATIONSHIP**

SCF control and Focal Document Element are unrelated; their content does not overlap.

X
SCF
SUBSET OF
Relative Relationship Strength (control versus control)
INTERSECTS WITH
Relative Relationship Strength (control versus control)
EQUAL
Relative Relationship Strength (control versus control)
SUPERSET OF
Relative Relationship Strength (control versus control)
NO RELATIONSHIP
Relative Relationship Strength (control versus control)
STRONG (10)
MODERATE (5)
NOMINAL (1)
EQUAL COVERAGE (10)
NONE (NOT APPLICABLE)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.1.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.1[a]	N/A	authorized users are identified.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
3.1.1[b]	N/A	processes acting on behalf of authorized users are identified.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
3.1.1[c]	N/A	devices (including other systems) authorized to connect to the system are identified.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
3.1.1[d]	N/A	system access is limited to authorized users.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
3.1.1[e]	N/A	system access is limited to processes acting on behalf of authorized users.	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
3.1.1[f]	N/A	system access is limited to authorized devices (including other systems).	Functional	Intersects With	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5	
3.1.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.2[a]	N/A	the types of transactions and functions that authorized users are permitted to execute are defined	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
3.1.2[b]	N/A	system access is limited to the defined types of transactions and functions for authorized users.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
3.1.3	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.3[a]	N/A	information flow control policies are defined.	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	
3.1.3[b]	N/A	methods and enforcement mechanisms for controlling the flow of CUI are defined.	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	
3.1.3[c]	N/A	designated sources and destinations (e.g., networks, individuals, and devices) for CUI within systems and between interconnected systems are identified.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
				Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
				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	
3.1.3[d]	N/A	authorizations for controlling the flow of CUI are defined.	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	
3.1.3[e]	N/A	approved authorizations for controlling the flow of CUI are enforced.	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	
3.1.4	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.4[a]	N/A	the duties of individuals requiring separation to reduce the risk of malevolent activity are defined.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	7	
3.1.4[b]	N/A	organization-defined duties of individuals requiring separation are separated.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	7	
3.1.4[c]	N/A	separate accounts for individuals whose duties and accesses must be separated to reduce the risk of malevolent activity or collusion are established	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	7	
3.1.5	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.5[a]	N/A	privileged accounts are identified.	Functional	Intersects With	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.	5	
3.1.5[b]	N/A	access to privileged accounts is authorized in accordance with the principle of least privilege.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
3.1.5[c]	N/A	security functions are identified.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
3.1.5[d]	N/A	access to security functions is authorized in accordance with the principle of least privilege.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
3.1.6	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.6[a]	N/A	nonsecurity functions are identified.	Functional	Intersects With	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	5	
3.1.6[b]	N/A	users are required to use non-privileged accounts or roles when accessing nonsecurity functions.	Functional	Intersects With	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	5	
3.1.7	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.7[a]	N/A	privileged functions are defined.	Functional	Intersects With	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	5	
3.1.7[b]	N/A	non-privileged users are defined.	Functional	Intersects With	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	5	
3.1.7[c]	N/A	non-privileged users are prevented from executing privileged functions.	Functional	Intersects With	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	5	
3.1.7[d]	N/A	the execution of privileged functions is captured in audit logs.	Functional	Intersects With	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	5	
3.1.8	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.8[a]	N/A	the means of limiting unsuccessful logon attempts is defined.	Functional	Intersects With	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	
3.1.8[b]	N/A	the defined means of limiting unsuccessful logon attempts is implemented.	Functional	Intersects With	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	
3.1.9	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.9[a]	N/A	privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category	Functional	Intersects With	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 the system that provides cybersecurity & data privacy notices.	5	
				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 that provides cybersecurity & data privacy notices.	5	
				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 source, such as Active Directory.	5	
		privacy and security notices are displayed.		Intersects With	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 the system that provides cybersecurity & data privacy notices.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.1.9[b]	N/A		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 that provides cybersecurity & data privacy notices.	5	
				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 source, such as Active Directory.	5	
3.1.10	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.10[a]	N/A	the period of inactivity after which the system initiates a session lock is defined.	Functional	Intersects With	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.	5	
3.1.10[b]	N/A	access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity.	Functional	Intersects With	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.	5	
3.1.10[c]	N/A	previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.	Functional	Intersects With	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.	5	
3.1.11	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.11[a]	N/A	conditions requiring a user session to terminate are defined.	Functional	Intersects With	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.	5	
3.1.11[b]	N/A	a user session is automatically terminated after any of the defined conditions occur.	Functional	Intersects With	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.	5	
3.1.12	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.12[a]	N/A	remote access sessions are permitted.	Functional	Intersects With	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	5	
3.1.12[b]	N/A	the types of permitted remote access are identified.	Functional	Intersects With	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	5	
3.1.12[c]	N/A	remote access sessions are controlled.	Functional	Intersects With	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	5	
3.1.12[d]	N/A	remote access sessions are monitored.	Functional	Intersects With	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.	5	
3.1.13	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.13[a]	N/A	cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.	Functional	Intersects With	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	5	
3.1.13[b]	N/A	cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.	Functional	Intersects With	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	5	
3.1.14	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.14[a]	N/A	managed access control points are identified and implemented.	Functional	Intersects With	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	5	
3.1.14[b]	N/A	remote access is routed through managed network access control points.	Functional	Intersects With	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	5	
3.1.15	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.15[a]	N/A	privileged commands authorized for remote execution are identified.	Functional	Intersects With	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	5	
3.1.15[b]	N/A	security-relevant information authorized to be accessed remotely is identified.	Functional	Intersects With	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	5	
3.1.15[c]	N/A	the execution of the identified privileged commands via remote access is authorized.	Functional	Intersects With	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	5	
3.1.15[d]	N/A	access to the identified security-relevant information via remote access is authorized.	Functional	Intersects With	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	5	
3.1.16	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.16[a]	N/A	wireless access points are identified.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
3.1.16[b]	N/A	wireless access is authorized prior to allowing such connections.	Functional	Intersects With	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5	
3.1.17	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.17[a]	N/A	wireless access to the system is protected using encryption.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to protect wireless access through authentication and strong encryption.	5	
3.1.17[b]	N/A	wireless access to the system is protected using authentication.	Functional	Intersects With	Authentication & Encryption	NET-15.1	Mechanisms exist to protect wireless access through authentication and strong encryption.	5	
3.1.18	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.18[a]	N/A	mobile devices that process, store, or transmit CUI are identified.	Functional	Intersects With	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational systems.	5	
3.1.18[b]	N/A	the connection of mobile devices is authorized.	Functional	Intersects With	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational systems.	5	
3.1.18[c]	N/A	mobile device connections are monitored and logged.	Functional	Intersects With	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational systems.	5	
3.1.19	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.19[a]	N/A	mobile devices and mobile computing platforms that process, store, or transmit CUI are identified.	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5	
3.1.19[b]	N/A	encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5	
3.1.20	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.20[a]	N/A	connections to external systems are identified.	Functional	Intersects With	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	5	
3.1.20[b]	N/A	use of external systems is identified.	Functional	Intersects With	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	5	
3.1.20[c]	N/A	connections to external systems are verified.	Functional	Intersects With	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	5	
3.1.20[d]	N/A	use of external systems is verified.	Functional	Intersects With	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	5	
3.1.20[e]	N/A	connections to external systems are controlled/limited.	Functional	Intersects With	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	5	
3.1.20[f]	N/A	use of external systems is controlled/limited.	Functional	Intersects With	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.	5	
3.1.21	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.21[a]	N/A	use of organizational portable storage devices containing CUI on external systems is identified and documented.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
3.1.21[b]	N/A	limits on the use of organizational portable storage devices containing CUI on external systems are defined.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
3.1.21[c]	N/A	use of organizational portable storage devices containing CUI on external systems is limited as defined.	Functional	Intersects With	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.	5	
3.1.22	N/A	Determine if CUI posted or processed on publicly accessible systems is controlled.	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.1.22[a]	N/A	individuals authorized to post or process information on publicly accessible systems are identified.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
				Intersects With	Sensitive Data In Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive/regulated data in public cloud providers.	5	
				Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.1.22[a]	N/A		Functional	Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports.	5	
				Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
3.1.22[b]	N/A	procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
				Intersects With	Sensitive Data In Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive/regulated data in public cloud providers.	5	
				Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
				Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports.	5	
				Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
3.1.22[c]	N/A	a review process in in place prior to posting of any content to publicly accessible systems.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
				Intersects With	Sensitive Data In Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive/regulated data in public cloud providers.	5	
				Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
				Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports.	5	
				Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
3.1.22[d]	N/A	content on publicly accessible information systems is reviewed to ensure that it does not include CUI.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
				Intersects With	Sensitive Data In Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive/regulated data in public cloud providers.	5	
				Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
				Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports.	5	
				Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
3.1.22[e]	N/A	mechanisms are in place to remove and address improper posting of CUI.	Functional	Intersects With	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	5	
				Intersects With	Sensitive Data In Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive/regulated data in public cloud providers.	5	
				Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
				Intersects With	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports.	5	
				Intersects With	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	5	
3.2.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.2.1[a]	N/A	security risks associated with organizational activities involving CUI are identified.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
3.2.1[b]	N/A	policies, standards, and procedures related to the security of the system are identified.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
3.2.1[c]	N/A	managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
3.2.1[d]	N/A	managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.	Functional	Intersects With	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
3.2.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.2.2[a]	N/A	information security-related duties, roles, and responsibilities are defined.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
				Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
3.2.2[b]	N/A	information security-related duties, roles, and responsibilities are assigned to designated personnel.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
				Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
3.2.2[c]	N/A	personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
				Intersects With	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
3.2.3	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.2.3[a]	N/A	potential indicators associated with insider threats are identified.	Functional	Intersects With	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	5	
3.2.3[b]	N/A	security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.	Functional	Intersects With	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	5	
3.3.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.3.1[a]	N/A	audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.3.1[b]	N/A	the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
3.3.1[c]	N/A	audit records are created (generated).	Functional	Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
3.3.1[d]	N/A	audit records, once created, contain the defined content.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
3.3.1[e]	N/A	retention requirements for audit records are defined.	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.	5	
3.3.1[f]	N/A	audit records are retained as defined.	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.	5	
3.3.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.3.2[a]	N/A	the content of the audit records needed to support the ability to uniquely trace users to their actions is defined.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
				Intersects With	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
				Intersects With	Database Logging	MON-03.7	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	5	
3.3.2[b]	N/A	audit records, once created, contain the defined content.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
3.3.3	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.3.3[a]	N/A	a process for determining when to review logged events is defined.	Functional	Intersects With	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
3.3.3[b]	N/A	event types being logged are reviewed in accordance with the defined review process.	Functional	Intersects With	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
3.3.3[c]	N/A	event types being logged are updated based on the review.	Functional	Intersects With	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
3.3.4	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.3.4[a]	N/A	personnel or roles to be alerted in the event of an audit logging process failure are identified.	Functional	Intersects With	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.	5	
3.3.4[b]	N/A	types of audit logging process failures for which alert will be generated are defined.	Functional	Intersects With	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.	5	
3.3.4[c]	N/A	identified personnel or roles are alerted in the event of an audit logging process failure.	Functional	Intersects With	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.	5	
3.3.5	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.3.5[a]	N/A	audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
3.3.5[b]	N/A	defined audit record review, analysis, and reporting processes are correlated.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
3.3.6	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.3.6[a]	N/A	an audit record reduction capability that supports on-demand analysis is provided.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
3.3.6[b]	N/A	a report generation capability that supports on-demand reporting is provided.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
3.3.7	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.3.7[a]	N/A	internal system clocks are used to generate time stamps for audit records.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure systems to use an authoritative time source to generate time stamps for event logs.	5	
3.3.7[b]	N/A	an authoritative source with which to compare and synchronize internal system clocks is specified.	Functional	Intersects With	Time Stamps	MON-07	Mechanisms exist to configure systems to use an authoritative time source to generate time stamps for event logs.	5	
				Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	
3.3.7[c]	N/A	internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	
3.3.8	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.3.8[a]	N/A	audit information is protected from unauthorized access.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
3.3.8[b]	N/A	audit information is protected from unauthorized modification.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
3.3.8[c]	N/A	audit information is protected from unauthorized deletion.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
3.3.8[d]	N/A	audit logging tools are protected from unauthorized access.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
3.3.8[e]	N/A	audit logging tools are protected from unauthorized modification.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
3.3.8[f]	N/A	audit logging tools are protected from unauthorized deletion.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	5	
3.3.9	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.3.9[a]	N/A	a subset of privileged users granted access to manage audit logging functionality is defined.	Functional	Intersects With	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.	5	
3.3.9[b]	N/A	management of audit logging functionality is limited to the defined subset of privileged users.	Functional	Intersects With	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.	5	
3.4.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.4.1[a]	N/A	a baseline configuration is established.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
				Subset Of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	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 (optional)	Notes (optional)
3.4.1[b]	N/A	the baseline configuration includes hardware, software, firmware, and documentation.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
				Subset Of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	
3.4.1[c]	N/A	the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
				Subset Of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	
3.4.1[d]	N/A	a system inventory is established.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
3.4.1[e]	N/A	the system inventory includes hardware, software, firmware, and documentation.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
3.4.1[f]	N/A	the inventory is maintained (reviewed and updated) throughout the system development life cycle.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
				Intersects With	Updates During Installations / Removals	AST-02.1	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
3.4.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.4.2[a]	N/A	security configuration settings for information technology products employed in the system are established and included in the baseline configuration.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
				Subset Of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	
3.4.2[b]	N/A	security configuration settings for information technology products employed in the system are enforced.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
				Subset Of	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	10	
3.4.3	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.4.3[a]	N/A	changes to the system are tracked.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
3.4.3[b]	N/A	changes to the system are reviewed.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
3.4.3[c]	N/A	changes to the system are approved or disapproved.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
3.4.3[d]	N/A	changes to the system are logged.	Functional	Intersects With	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
3.4.4	N/A	Determine if the security impact of changes to each organizational system is analyzed prior to implementation.	Functional	Intersects With	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
3.4.5	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.4.5[a]	N/A	physical access restrictions associated with changes to the system are defined.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
			Functional	Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to systems.	5	
3.4.5[b]	N/A	physical access restrictions associated with changes to the system are documented.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
				Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to systems.	5	
3.4.5[c]	N/A	physical access restrictions associated with changes to the system are approved.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
				Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to systems.	5	
3.4.5[d]	N/A	physical access restrictions associated with changes to the system are enforced.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
				Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to systems.	5	
3.4.5[e]	N/A	logical access restrictions associated with changes to the system are defined.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
				Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to systems.	5	
3.4.5[f]	N/A	logical access restrictions associated with changes to the system are documented.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
				Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to systems.	5	
3.4.5[g]	N/A	logical access restrictions associated with changes to the system are approved.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
				Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to systems.	5	
3.4.5[h]	N/A	logical access restrictions associated with changes to the system are enforced.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
				Intersects With	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to systems.	5	
3.4.6	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.4.6[a]	N/A	essential system capabilities are defined based on the principle of least functionality.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
3.4.6[b]	N/A	the system is configured to provide only the defined essential capabilities.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
3.4.7	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.4.7[a]	N/A	essential programs are defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[b]	N/A	the use of nonessential programs is defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[c]	N/A	the use of nonessential programs is restricted, disabled, or prevented as defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[d]	N/A	essential functions are defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[e]	N/A	the use of nonessential functions is defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[f]	N/A	the use of nonessential functions is restricted, disabled, or prevented as defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[g]	N/A	essential ports are defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[h]	N/A	the use of nonessential ports is defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[i]	N/A	the use of nonessential ports is restricted, disabled, or prevented as defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.4.7[j]	N/A	essential protocols are defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[k]	N/A	the use of nonessential protocols is defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[l]	N/A	the use of nonessential protocols is restricted, disabled, or prevented as defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[m]	N/A	essential services are defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[n]	N/A	the use of nonessential services is defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.7[o]	N/A	the use of nonessential services is restricted, disabled, or prevented as defined.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
3.4.8	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.4.8[a]	N/A	a policy specifying whether whitelisting or blacklisting is to be implemented is specified.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
3.4.8[b]	N/A	the software allowed to execute under whitelisting or denied use under blacklisting is specified.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
3.4.8[c]	N/A	whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
3.4.9	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.4.9[a]	N/A	a policy for controlling the installation of software by users is established.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
3.4.9[b]	N/A	installation of software by users is controlled based on the established policy.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
3.4.9[c]	N/A	installation of software by users is monitored.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
3.5.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.5.1[a]	N/A	system users are identified.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
3.5.1[b]	N/A	processes acting on behalf of users are identified.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
3.5.1[c]	N/A	devices accessing the system are identified.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
3.5.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.5.2[a]	N/A	the identity of each user is authenticated or verified as a prerequisite to system access.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
3.5.2[b]	N/A	the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
3.5.2[c]	N/A	the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
3.5.3	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.5.3[a]	N/A	privileged accounts are identified.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
				Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
3.5.3[b]	N/A	multifactor authentication is implemented for local access to privileged accounts.	Functional	Intersects With	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5	
3.5.3[c]	N/A	multifactor authentication is implemented for network access to privileged accounts.	Functional	Intersects With	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5	
3.5.3[d]	N/A	multifactor authentication is implemented for network access to non-privileged accounts.	Functional	Intersects With	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	5	
3.5.4	N/A	Determine if replay-resistant authentication mechanisms are implemented for all network account access to privileged and non-privileged accounts.	Functional	Intersects With	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	5	
3.5.5	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.5.5[a]	N/A	a period within which identifiers cannot be reused is defined.	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and systems.	5	
3.5.5[b]	N/A	reuse of identifiers is prevented within the defined period.	Functional	Intersects With	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and systems.	5	
3.5.6	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.5.6[a]	N/A	a period of inactivity after which an identifier is disabled is defined.	Functional	Intersects With	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5	
3.5.6[b]	N/A	identifiers are disabled after the defined period of inactivity.	Functional	Intersects With	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5	
3.5.7	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.5.7[a]	N/A	password complexity requirements are defined.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
3.5.7[b]	N/A	password change of character requirements are defined.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
3.5.7[c]	N/A	minimum password complexity requirements as defined are enforced when new passwords are created.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
3.5.7[d]	N/A	minimum password change of character requirements as defined are enforced when new passwords are created.	Functional	Intersects With	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
3.5.8	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.5.8[a]	N/A	the number of generations during which a password cannot be reused is specified.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	
3.5.8[b]	N/A	reuse of passwords is prohibited during the specified number of generations.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	
3.5.9	N/A	Determine if an immediate change to a permanent password is required when a temporary password is used for system logon.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	
3.5.10	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.5.10[a]	N/A	passwords are cryptographically protected in storage.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
3.5.10[b]	N/A	passwords are cryptographically protected in transit.	Functional	Intersects With	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
3.5.11	N/A	Determine if authentication information is obscured during the authentication process.	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	
3.6.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
		an operational incident-handling capability is established.		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 & data privacy-related incidents.	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 (optional)	Notes (optional)
3.6.1[a]	N/A		Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.1[b]	N/A	the operational incident-handling capability includes preparation.	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 & data privacy-related incidents.	10	
				Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.1[c]	N/A	the operational incident-handling capability includes detection.	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 & data privacy-related incidents.	10	
				Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.1[d]	N/A	the operational incident-handling capability includes analysis.	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 & data privacy-related incidents.	10	
				Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.1[e]	N/A	the operational incident-handling capability includes containment.	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 & data privacy-related incidents.	10	
				Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.1[f]	N/A	the operational incident-handling capability includes recovery.	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 & data privacy-related incidents.	10	
				Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.1[g]	N/A	the operational incident-handling capability includes user response activities.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.6.2[a]	N/A	incidents are tracked.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.2[b]	N/A	incidents are documented.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.2[c]	N/A	authorities to whom incidents are to be reported are identified.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.2[d]	N/A	organizational officials to whom incidents are to be reported are identified.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.2[e]	N/A	identified authorities are notified of incidents.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3.6.2[f]	N/A	identified organizational officials are notified of incidents.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.6.3	N/A	Determine if the incident response capability is tested.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
3.7.1	N/A	Determine if system maintenance is performed.	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service.	5	
3.7.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.7.2[a]	N/A	tools used to conduct system maintenance are controlled.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
3.7.2[b]	N/A	techniques used to conduct system maintenance are controlled.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
3.7.2[c]	N/A	mechanisms used to conduct system maintenance are controlled.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
3.7.2[d]	N/A	personnel used to conduct system maintenance are controlled.	Functional	Intersects With	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	5	
3.7.3	N/A	Determine if equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
3.7.4	N/A	Determine if media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.	Functional	Intersects With	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	5	
3.7.5	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.7.5[a]	N/A	multifactor authentication is required to establish nonlocal maintenance sessions via external network connections.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	
3.7.5[b]	N/A	nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	
3.7.6	N/A	Determine if maintenance personnel without required access authorization are supervised during maintenance activities.	Functional	Intersects With	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	5	
3.8.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.8.1[a]	N/A	paper media containing CUI is physically controlled.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
3.8.1[b]	N/A	digital media containing CUI is physically controlled.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
3.8.1[c]	N/A	paper media containing CUI is securely stored.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
3.8.1[d]	N/A	digital media containing CUI is securely stored.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
3.8.2	N/A	Determine if access to CUI on system media is limited to authorized users.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
3.8.3	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.8.3[a]	N/A	system media containing CUI is sanitized or destroyed before disposal.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
3.8.3[b]	N/A	system media containing CUI is sanitized before it is released for reuse.	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	5	
3.8.4	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.8.4[a]	N/A	media containing CUI is marked with applicable CUI markings.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
3.8.4[b]	N/A	media containing CUI is marked with distribution limitations.	Functional	Intersects With	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.	5	
3.8.5	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.8.5[a]	N/A	access to media containing CUI is controlled.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
3.8.5[b]	N/A	accountability for media containing CUI is maintained during transport outside of controlled areas.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
3.8.6	N/A	Determine if the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
3.8.7	N/A	Determine if the use of removable media on system components containing CUI is controlled.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
3.8.8	N/A	Determine if the use of portable storage devices is prohibited when such devices have no identifiable owner.	Functional	Intersects With	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational information systems when such devices have no identifiable owner.	5	
3.8.9	N/A	Determine if the confidentiality of backup CUI is protected at storage locations.	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
				Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
3.9.1	N/A	Determine if individuals are screened prior to authorizing access to organizational systems.	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
3.9.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.9.2[a]	N/A	a policy and/or process for terminating system access authorization and any credentials coincident with personnel actions is established.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
				Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
				Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
				Intersects With	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to systems and facilities upon personnel reassignment or transfer, in a timely manner.	5	
				Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
3.9.2[b]	N/A	system access and credentials are terminated consistent with personnel actions such as termination or transfer.	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
				Intersects With	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to systems and facilities upon personnel reassignment or transfer, in a timely manner.	5	
				Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
3.9.2[c]	N/A	the system is protected during and after personnel transfer actions.	Functional	Intersects With	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
				Intersects With	Personnel Transfer	HRS-08	Mechanisms exist to adjust logical and physical access authorizations to systems and facilities upon personnel reassignment or transfer, in a timely manner.	5	
				Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
3.10.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.10.1[a]	N/A	authorized individuals allowed physical access are identified.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
3.10.1[b]	N/A	physical access to organizational systems is limited to authorized individuals.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.10.1[c]	N/A	physical access to equipment is limited to authorized individuals.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
3.10.1[d]	N/A	physical access to operating environments is limited to authorized individuals.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
3.10.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.10.2[a]	N/A	the physical facility where that system resides is protected.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
3.10.2[b]	N/A	the support infrastructure for that system is protected.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
3.10.2[c]	N/A	the physical facility where that system resides is monitored.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
				Subset Of	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
				Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	
				Intersects With	Monitoring Physical Access To Information Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical information systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.		
3.10.2[d]	N/A	the support infrastructure for that system is monitored.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
				Subset Of	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
				Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	
				Intersects With	Monitoring Physical Access To Information Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical information systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.	5	
3.10.3	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.10.3[a]	N/A	visitors are escorted.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
				Intersects With	Distinguish Visitors from On-Site Personnel	PES-06.1	Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible.	5	
				Intersects With	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	
3.10.3[b]	N/A	visitor activity is monitored.	Functional	Intersects With	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	5	
				Intersects With	Distinguish Visitors from On-Site Personnel	PES-06.1	Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible.	5	
				Intersects With	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.	5	
3.10.4	N/A	Determine if audit logs of physical access are maintained.	Functional	Intersects With	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	
3.10.5	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.10.5[a]	N/A	physical access devices are identified.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
3.10.5[b]	N/A	physical access devices are controlled.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
3.10.5[c]	N/A	physical access devices are managed.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
3.10.6	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.10.6[a]	N/A	safeguarding measures for CUI are defined for alternate work sites.	Functional	Intersects With	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	5	
3.10.6[b]	N/A	safeguarding measures for CUI are enforced for alternate work sites.	Functional	Intersects With	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	5	
3.11.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.11.1[a]	N/A	the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
3.11.1[b]	N/A	risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
3.11.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.11.2[a]	N/A	the frequency to scan for vulnerabilities in an organizational system and its applications that process, store, or transmit CUI is defined.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
3.11.2[b]	N/A	vulnerability scans are performed in an organizational system that processes, stores, or transmits CUI with the defined frequency.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
3.11.2[c]	N/A	vulnerability scans are performed in an application that contains CUI with the defined frequency.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
3.11.2[d]	N/A	vulnerability scans are performed in an organizational system that processes, stores, or transmits CUI when new vulnerabilities are identified.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
3.11.2[e]	N/A	vulnerability scans are performed in an application that contains CUI when new vulnerabilities are identified.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
3.11.3	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.11.3[a]	N/A	vulnerabilities are identified.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
3.11.3[b]	N/A	vulnerabilities are remediated in accordance with risk assessments.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
3.12.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.12.1[a]	N/A	the frequency of security control assessments is defined.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
3.12.1[b]	N/A	security controls are assessed with the defined frequency to determine if the controls are effective in their application.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
3.12.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.12.2[a]	N/A	deficiencies and vulnerabilities to be addressed by the plan of action are identified.	Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.12.2[b]	N/A	a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.	Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
3.12.2[c]	N/A	the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.	Functional	Intersects With	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
3.12.3	N/A	Determine if security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.	Functional	Intersects With	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
3.12.4	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.12.4[a]	N/A	a system security plan is developed.	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
3.12.4[b]	N/A	the system boundary is described and documented in the system security plan.	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
3.12.4[c]	N/A	the system environment of operation is described and documented in the system security plan.	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
3.12.4[d]	N/A	the security requirements identified and approved by the designated authority as non-applicable are identified.	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
3.12.4[e]	N/A	the method of security requirement implementation is described and documented in the system security plan.	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
3.12.4[f]	N/A	the relationship with or connection to other systems is described and documented in the system security plan.	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
3.12.4[g]	N/A	the frequency to update the system security plan is defined.	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
3.12.4[h]	N/A	system security plan is updated with the defined frequency.	Functional	Intersects With	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	5	
3.13.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.1[a]	N/A	the external system boundary is defined.	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	
3.13.1[b]	N/A	key internal system boundaries are defined.	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	
3.13.1[c]	N/A	communications are monitored at the external system boundary.	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	
3.13.1[d]	N/A	communications are monitored at key internal boundaries.	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	
3.13.1[e]	N/A	communications are controlled at the external system boundary.	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	
				Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	
3.13.1[f]	N/A	communications are controlled at key internal boundaries.	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	
3.13.1[g]	N/A	communications are protected at the external system boundary.	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	
				Intersects With	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.	5	
3.13.1[h]	N/A	communications are protected at key internal boundaries.	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	
3.13.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.2[a]	N/A	architectural designs that promote effective information security are identified.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
3.13.2[b]	N/A	software development techniques that promote effective information security are identified.	Functional	Intersects With	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
3.13.2[c]	N/A	systems engineering principles that promote effective information security are identified.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
3.13.2[d]	N/A	identified architectural designs that promote effective information security are employed.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
3.13.2[e]	N/A	identified software development techniques that promote effective information security are employed.	Functional	Intersects With	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
3.13.2[f]	N/A	identified systems engineering principles that promote effective information security are employed.	Functional	Subset Of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
3.13.3	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.3[a]	N/A	user functionality is identified.	Functional	Intersects With	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	5	
3.13.3[b]	N/A	system management functionality is identified.	Functional	Intersects With	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	5	
3.13.3[c]	N/A	user functionality is separated from system management functionality.	Functional	Intersects With	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	5	
3.13.4	N/A	Determine if unauthorized and unintended information transfer via shared system resources is prevented.	Functional	Intersects With	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.13.5	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.5[a]	N/A	publicly accessible system components are identified.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
3.13.5[b]	N/A	subnetworks for publicly accessible system components are physically or logically separated from internal networks.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
3.13.6	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.6[a]	N/A	network communications traffic is denied by default.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
3.13.6[b]	N/A	network communications traffic is allowed by exception.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).	5	
3.13.7	N/A	Determine if remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).	Functional	Intersects With	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	5	
3.13.8	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.8[a]	N/A	cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.	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	
				Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
3.13.8[b]	N/A	alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.	Functional	Intersects With	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	5	
3.13.8[c]	N/A	either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.	Functional	Intersects With	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	5	
3.13.9	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.9[a]	N/A	a period of inactivity to terminate network connections associated with communications sessions is defined.	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	
3.13.9[b]	N/A	network connections associated with communications sessions are terminated at the end of the sessions.	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	
3.13.9[c]	N/A	network connections associated with communications sessions are terminated after the defined period of inactivity.	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	
3.13.10	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.10[a]	N/A	cryptographic keys are established whenever cryptography is employed.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
				Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
3.13.10[b]	N/A	cryptographic keys are managed whenever cryptography is employed.	Functional	Intersects With	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	5	
				Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
3.13.11	N/A	Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI.	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	
				Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
3.13.12	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.12[a]	N/A	collaborative computing devices are identified.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	5	
3.13.12[b]	N/A	collaborative computing devices provide indication to users of devices in use.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	5	
3.13.12[c]	N/A	remote activation of collaborative computing devices is prohibited.	Functional	Intersects With	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: (1) Networked whiteboards; (2) Video teleconference cameras; and (3) Teleconference microphones.	5	
3.13.13	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.13[a]	N/A	use of mobile code is controlled.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
3.13.13[b]	N/A	use of mobile code is monitored.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	
3.13.14	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.13.14[a]	N/A	use of Voice over Internet Protocol (VoIP) technologies is controlled.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
3.13.14[b]	N/A	use of Voice over Internet Protocol (VoIP) technologies is monitored.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
3.13.15	N/A	Determine if the authenticity of communications sessions is protected.	Functional	Intersects With	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5	
3.13.16	N/A	Determine if the confidentiality of CUI at rest is protected.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
3.14.1	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.14.1[a]	N/A	the time within which to identify system flaws is specified.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.14.1[b]	N/A	system flaws are identified within the specified time frame.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.14.1[c]	N/A	the time within which to report system flaws is specified.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.14.1[d]	N/A	system flaws are reported within the specified time frame.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.14.1[e]	N/A	the time within which to correct system flaws is specified.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.14.1[f]	N/A	system flaws are corrected within the specified time frame.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
3.14.2	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.14.2[a]	N/A	designated locations for malicious code protection are identified.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
3.14.2[b]	N/A	protection from malicious code at designated locations is provided.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
3.14.3	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.14.3[a]	N/A	response actions to system security alerts and advisories are identified.	Functional	Intersects With	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.14.3[b]	N/A	system security alerts and advisories are monitored.	Functional	Intersects With	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
3.14.3[c]	N/A	actions in response to system security alerts and advisories are taken.	Functional	Intersects With	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
3.14.4	N/A	Determine if malicious code protection mechanisms are updated when new releases are available.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	5	
3.14.5	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.14.5[a]	N/A	the frequency for malicious code scans is defined.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
3.14.5[b]	N/A	malicious code scans are performed with the defined frequency.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
3.14.5[c]	N/A	real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
				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.	5	
3.14.6	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.14.6[a]	N/A	the system is monitored to detect attacks and indicators of potential attacks.	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.	5	
3.14.6[b]	N/A	inbound communications traffic is monitored to detect attacks and indicators of potential attacks.	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.	5	
3.14.6[c]	N/A	outbound communications traffic is monitored to detect attacks and indicators of potential attacks.	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.	5	
3.14.7	N/A	Determine If:	Functional	No Relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3.14.7[a]	N/A	authorized use of the system is defined.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
3.14.7[b]	N/A	unauthorized use of the system is identified.	Functional	Intersects With	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	