NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference document: Secure Controls Framework (SCF) version 2025.4
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: Center for Internet Security (CIS) Critical Security Controls (CSC) version 8.1 - IG1
Focal Document URL: https://www.cisecurity.org/controls/v8-1
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-general-cis-csc-8-1-ig1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	Functional	Equal	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	10	
1.2	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Functional	Intersects With	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	5	
1.2	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	Functional	Intersects With	Host Containment	NET-08.3	Automated mechanisms exist to enforce host containment protections that revoke or quarantine a host's access to the network.	5	
2.1	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
2.1	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
2.1	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
2.2	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Functional	Subset Of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
2.2	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
2.2	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Functional	Intersects With	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	5	
2.2	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
2.2	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5	
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Functional	Intersects With	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	5	
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Functional	Intersects With	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	5	
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	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	
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Functional	Intersects With	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	5	
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Functional	Intersects With	Integrity Assurance & Enforcement (IAE)	CFG-06.1	Automated mechanisms exist to identify unauthorized deviations from an approved baseline and implement automated resiliency actions to remediate the unauthorized change.	5	
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Functional	Intersects With	Unauthorized Activities	MON-16.3	Mechanisms exist to monitor for unauthorized activities, accounts, connections, devices and software.	5	
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Functional	Intersects With	Software Installation Alerts	END-03.1	Mechanisms exist to generate an alert when new software is detected.	5	
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	5	
2.3	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	Functional	Intersects With	Incident Handling	IRO-02	(2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment;	5	
3.1	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
3.1	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
3.1	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	
3.1	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	5	
3.1	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
3.1	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
3.1	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	5	
3.1	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
3.1	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
3.1	Establish and Maintain a Data Management Process	Establish and maintain a documented data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	5	
3.2	Establish and Maintain a Data Inventory	Establish and maintain a data inventory based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
3.2	Establish and Maintain a Data Inventory	Establish and maintain a data inventory based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.	Functional	Intersects With	Periodic Scans for Sensitive / Regulated Data	DCH-06.3	Mechanisms exist to periodically scan unstructured data sources for sensitive/regulated data or data requiring special protection measures by statutory, regulatory or contractual obligations.	5	
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	5	
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Functional	Intersects With	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive/regulated data to authorized parties with a need to know.	5	
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Functional	Intersects With	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, including Technology Assets, Applications and/or Services (TAAS), from storing, processing and transmitting data unless authorized individuals first: (1) Verifying the implementation of required security, compliance and/or resilience controls; or (2) Retaining a processing agreement with the entity hosting the external TAAS.	5	
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Functional	Intersects With	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	5	
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Functional	Intersects With	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or Technology Assets, Applications and/or Services (TAAS) transferring data between interconnecting TAAS have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.	5	
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Functional	Intersects With	Data Access Mapping	DCH-14.3	Mechanisms exist to leverage data-specific Access Control Lists (ACL) or Interconnection Security Agreements (ISAs) to generate a logical map of the parties with whom sensitive/regulated data is shared.	5	
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
3.3	Configure Data Access Control Lists	Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	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	
3.4	Enforce Data Retention	Retain data according to the enterprise's documented data management process. Data retention must include both minimum and maximum timelines.	Functional	Equal	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
3.5	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Functional	Intersects With	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
3.5	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Functional	Intersects With	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	5	
3.5	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	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	
3.5	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Functional	Intersects With	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	5	
3.5	Securely Dispose of Data	Securely dispose of data as outlined in the enterprise's documented data management process. Ensure the disposal process and method are commensurate with the data sensitivity.	Functional	Intersects With	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
3.6	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	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	
3.6	Encrypt Data on End-User Devices	Encrypt data on end-user devices containing sensitive data. Example implementations can include: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
4.1	Establish and Maintain a Secure Configuration Process	Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
4.1	Establish and Maintain a Secure Configuration Process	Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
4.1	Establish and Maintain a Secure Configuration Process	Establish and maintain a documented secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	Establish and maintain a documented secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
4.3	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
4.3	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	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	
4.4	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
4.4	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	Functional	Intersects With	Software Firewall	END-05	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all endpoint devices, where technically feasible.	5	
4.4	Implement and Manage a Firewall on Servers	Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	Functional	Intersects With	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	5	
4.5	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
4.5	Implement and Manage a Firewall on End-User Devices	Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	Functional	Intersects With	Software Firewall	END-05	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all endpoint devices, where technically feasible.	5	
4.6	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
4.6	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	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	
4.6	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	Functional	Intersects With	Non-Console Administrative Access	CRY-06	Cryptographic mechanisms exist to protect the confidentiality and integrity of non-console administrative access.	5	
4.6	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	
4.6	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	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	
4.6	Securely Manage Enterprise Assets and Software	Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled Infrastructure-as-Code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	Functional	Intersects With	Insecure Ports, Protocols & Services	TDA-02.6	Mechanisms exist to mitigate the risk associated with the use of insecure ports, protocols and services necessary to operate technology solutions.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
4.7	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
4.7	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
4.7	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
5.1	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory mustmust at a minimum include user, administrator accounts, and service accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
5.1	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory mustmust at a minimum include user, administrator accounts, and service accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	Functional	Intersects With	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	5	
5.2	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
5.2	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using Multi-Factor Authentication (MFA) and a 14-character password for accounts not using MFA.	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	
5.3	Disable Dormant Accounts	Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	Functional	Equal	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	10	
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	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	
5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	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	
6.1	Establish an Access Granting Process	Establish and follow a documented process, preferably automated, for granting access to enterprise assets upon new hire or role change of a user.	Functional	Equal	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	10	
6.2	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	Functional	Equal	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	10	
6.3	Require MFA for Externally-Exposed Applications	Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.	Functional	Equal	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	10	
6.4	Require MFA for Remote Network Access	Require MFA for remote network access.	Functional	Equal	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	10	
6.5	Require MFA for Administrative Access	Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a service provider.	Functional	Equal	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	10	
7.1	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
7.2	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.	Functional	Equal	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	10	
7.3	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Functional	Equal	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	10	
7.4	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
7.4	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	
7.4	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Functional	Intersects With	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	5	
7.4	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	Functional	Intersects With	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	5	
8.1	Establish and Maintain an Audit Log Management Process	Establish and maintain a documented audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
8.1	Establish and Maintain an Audit Log Management Process	Establish and maintain a documented audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
8.2	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
8.2	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5	
8.2	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
8.2	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Functional	Intersects With	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.	5	
8.2	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	Functional	Intersects With	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
8.3	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	Functional	Intersects With	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
8.3	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	Functional	Intersects With	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.	5	
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	Functional	Intersects With	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.	5	
9.1	Ensure Use of Only Fully Supported Browsers and Email Clients	Ensure only fully supported browsers and email clients are allowed to execute in the enterprise, only using the latest version of browsers and email clients provided through the vendor.	Functional	Intersects With	Restrict Roles Permitted To Install Software	CFG-05.2	Mechanisms exist to configure systems to prevent the installation of software, unless the action is performed by a privileged user or service.	5	
9.2	Use DNS Filtering Services	Use DNS filtering services on all end-user devices, including remote and on-premises assets, to block access to known malicious domains.	Functional	Equal	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	10	
10.1	Deploy and Maintain Anti-Malware Software	Deploy and maintain anti-malware software on all enterprise assets.	Functional	Equal	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
10.2	Configure Automatic Anti-Malware Signature Updates	Configure automatic updates for anti-malware signature files on all enterprise assets.	Functional	Equal	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	10	
10.3	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
10.3	Disable Autorun and Autoplay for Removable Media	Disable autorun and autoplay auto-execute functionality for removable media.	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	
11.1	Establish and Maintain a Data Recovery Process	Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
11.2	Perform Automated Backups	Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	Functional	Equal	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10	
11.3	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
11.3	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
11.3	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
11.3	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Functional	Intersects With	Backup & Restoration Hardware Protection	BCD-13	Mechanisms exist to protect backup and restoration hardware and software.	5	
11.3	Protect Recovery Data	Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
11.4	Establish and Maintain an Isolated Instance of Recovery Data	Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services.	Functional	Equal	Isolated Recovery Environment	BCD-14	Mechanisms exist to utilize an isolated, non-production environment to perform data backup and recovery operations through offline, cloud or off-site capabilities.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
12.1	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	Functional	Subset Of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
12.1	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	Functional	Intersects With	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	
12.1	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	Functional	Intersects With	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.	5	
12.1	Ensure Network Infrastructure is Up-to-Date	Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
14.1	Establish and Maintain a Security Awareness Program	Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Subset Of	Security, Compliance & Resilience-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
14.2	Train Workforce Members to Recognize Social Engineering Attacks	Train workforce members to recognize social engineering attacks, such as phishing, business email compromise (BEC), pretexting, and tailgating.	Functional	Equal	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	10	
14.3	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
14.3	Train Workforce Members on Authentication Best Practices	Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
14.4	Train Workforce on Data Handling Best Practices	Train workforce members on how to identify and properly store, transfer, archive, and destroy sensitive data. This also includes training workforce members on clear screen and desk best practices, such as locking their screen when they step away from their enterprise asset, erasing physical and virtual whiteboards at the end of meetings, and storing data and assets securely.	Functional	Equal	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	10	
14.5	Train Workforce Members on Causes of Unintentional Data Exposure	Train workforce members to be aware of causes for unintentional data exposure. Example topics include mis-delivery of sensitive data, losing a portable end-user device, or publishing data to unintended audiences.	Functional	Equal	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	10	
14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	Train workforce members to be able to recognize a potential incident and be able to report such an incident.	Functional	Equal	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	10	
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	Train workforce to understand how to verify and report out-of-date software patches or any failures in automated processes and tools. Part of this training should include notifying IT personnel of any failures in automated processes and tools.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5	
14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	Train workforce members on the dangers of connecting to, and transmitting data over, insecure networks for enterprise activities. If the enterprise has remote workers, training must include guidance to ensure that all users securely configure their home network infrastructure.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
15.1	Establish and Maintain an Inventory of Service Providers	Establish and maintain an inventory of service providers. The inventory is to list all known service providers, include classification(s), and designate an enterprise contact for each service provider. Review and update the inventory annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Equal	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	
17.1	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach. If using a service provider, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	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	
17.1	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach. If using a service provider, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
17.1	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, service providers, or a hybrid approach. If using a service provider, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5	
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	Functional	Intersects With	Vulnerabilities Related To Incidents	IRO-10.3	Mechanisms exist to report system vulnerabilities associated with reported cybersecurity and data protection incidents to organization-defined personnel or roles.	5	
17.2	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, service vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	Functional	Intersects With	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	
17.3	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an documented enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	Functional	Equal	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	