NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **CISA Cybersecurity Performance Goals (CPGs)**
Focal Document URL: https://www.cisa.gov/cybersecurity-performance-goals-cpgs
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-us-fed-dhs-cisa-cpg.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 (optional)	Notes (optional)
1.A	Asset Inventory	Better identify known, unknown (shadow), and unmanaged assets, and more rapidly detect and respond to new vulnerabilities.	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	Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.
1.A	Asset Inventory	Better identify known, unknown (shadow), and unmanaged assets, and more rapidly detect and respond to new vulnerabilities.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services 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	Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.
1.A	Asset Inventory	Better identify known, unknown (shadow), and unmanaged assets, and more rapidly detect and respond to new vulnerabilities.	Functional	Intersects With	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 systems, applications, services and data.	5	Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.
1.B	Organizational Cybersecurity Leadership	A single leader is responsible and accountable for cybersecurity within an organization.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning.
1.B	Organizational Cybersecurity Leadership	A single leader is responsible and accountable for cybersecurity within an organization.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning.
1.B	Organizational Cybersecurity Leadership	A single leader is responsible and accountable for cybersecurity within an organization.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning.
1.C	OT Cybersecurity Leadership	A single leader is responsible and accountable for OT-specific cybersecurity within an organization with OT assets.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations, this may be the same position as identified in 1.B.
1.C	OT Cybersecurity Leadership	A single leader is responsible and accountable for OT-specific cybersecurity within an organization with OT assets.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations, this may be the same position as identified in 1.B.
1.C	OT Cybersecurity Leadership	A single leader is responsible and accountable for OT-specific cybersecurity within an organization with OT assets.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations, this may be the same position as identified in 1.B.
1.D	Improving IT and OT Cybersecurity Relationships	Improve OT cybersecurity and more rapidly and effectively respond to OT cyber incidents.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Organizations sponsor at least one “pizza party” or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel and is not a working event (such as providing meals during an incident response).
1.D	Improving IT and OT Cybersecurity Relationships	Improve OT cybersecurity and more rapidly and effectively respond to OT cyber incidents.	Functional	Intersects With	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	5	Organizations sponsor at least one “pizza party” or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel and is not a working event (such as providing meals during an incident response).
1.D	Improving IT and OT Cybersecurity Relationships	Improve OT cybersecurity and more rapidly and effectively respond to OT cyber incidents.	Functional	Subset Of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	Organizations sponsor at least one “pizza party” or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel and is not a working event (such as providing meals during an incident response).
1.D	Improving IT and OT Cybersecurity Relationships	Improve OT cybersecurity and more rapidly and effectively respond to OT cyber incidents.	Functional	Intersects With	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	Organizations sponsor at least one “pizza party” or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel and is not a working event (such as providing meals during an incident response).
1.D	Improving IT and OT Cybersecurity Relationships	Improve OT cybersecurity and more rapidly and effectively respond to OT cyber incidents.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	Organizations sponsor at least one “pizza party” or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel and is not a working event (such as providing meals during an incident response).
1.D	Improving IT and OT Cybersecurity Relationships	Improve OT cybersecurity and more rapidly and effectively respond to OT cyber incidents.	Functional	Intersects With	Cybersecurity Knowledge Sharing	SAT-05	Mechanisms exist to improve cybersecurity and data protection knowledge sharing across security personnel allowing for more rapid and effective response to incidents.	5	Organizations sponsor at least one “pizza party” or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel and is not a working event (such as providing meals during an incident response).
1.D	Improving IT and OT Cybersecurity Relationships	Improve OT cybersecurity and more rapidly and effectively respond to OT cyber incidents.	Functional	Intersects With	Manage Organizational Knowledge	PRM-08	Mechanisms exist to manage the organizational knowledge of the cybersecurity & data privacy staff.	5	Organizations sponsor at least one “pizza party” or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel and is not a working event (such as providing meals during an incident response).
1.E	Mitigating Known Vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks.	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	All known exploited vulnerabilities (listed in CISA’s Known Exploited Vulnerabilities Catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first. OT: For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.
1.E	Mitigating Known Vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks.	Functional	Intersects With	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	All known exploited vulnerabilities (listed in CISA’s Known Exploited Vulnerabilities Catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first. OT: For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.
1.E	Mitigating Known Vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks.	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	All known exploited vulnerabilities (listed in CISA’s Known Exploited Vulnerabilities Catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first. OT: For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.
1.E	Mitigating Known Vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	All known exploited vulnerabilities (listed in CISA’s Known Exploited Vulnerabilities Catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first. OT: For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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)
1.E	Mitigating Known Vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	All known exploited vulnerabilities (listed in CISA's Known Exploited Vulnerabilities Catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first. OT: For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.
1.E	Mitigating Known Vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	All known exploited vulnerabilities (listed in CISA's Known Exploited Vulnerabilities Catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first. OT: For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.
1.E	Mitigating Known Vulnerabilities	Reduce the likelihood of threat actors exploiting known vulnerabilities to breach organizational networks.	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	All known exploited vulnerabilities (listed in CISA's Known Exploited Vulnerabilities Catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first. OT: For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.
1.F	Third-Party Validation of Cybersecurity Control Effectiveness	Identify TTPs that lack proper defenses and establish confidence in organizational cyber defenses.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.
1.F	Third-Party Validation of Cybersecurity Control Effectiveness	Identify TTPs that lack proper defenses and establish confidence in organizational cyber defenses.	Functional	Intersects With	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the data and systems under review.	5	Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.
1.F	Third-Party Validation of Cybersecurity Control Effectiveness	Identify TTPs that lack proper defenses and establish confidence in organizational cyber defenses.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.
1.F	Third-Party Validation of Cybersecurity Control Effectiveness	Identify TTPs that lack proper defenses and establish confidence in organizational cyber defenses.	Functional	Intersects With	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Automonous Technologies (AAT).	5	Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.
1.F	Third-Party Validation of Cybersecurity Control Effectiveness	Identify TTPs that lack proper defenses and establish confidence in organizational cyber defenses.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.
1.F	Third-Party Validation of Cybersecurity Control Effectiveness	Identify TTPs that lack proper defenses and establish confidence in organizational cyber defenses.	Functional	Intersects With	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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)
1.F	Third-Party Validation of Cybersecurity Control Effectiveness	Identify TTPs that lack proper defenses and establish confidence in organizational cyber defenses.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.
1.F	Third-Party Validation of Cybersecurity Control Effectiveness	Identify TTPs that lack proper defenses and establish confidence in organizational cyber defenses.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.
1.G	Supply Chain Incident Reporting	Organizations more rapidly learn about and respond to known incidents or breaches across vendors and service providers.	Functional	Subset Of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame as determined by the organization.
1.G	Supply Chain Incident Reporting	Organizations more rapidly learn about and respond to known incidents or breaches across vendors and service providers.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame as determined by the organization.
1.G	Supply Chain Incident Reporting	Organizations more rapidly learn about and respond to known incidents or breaches across vendors and service providers.	Functional	Intersects With	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 systems, applications, services and data.	5	Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame as determined by the organization.
1.G	Supply Chain Incident Reporting	Organizations more rapidly learn about and respond to known incidents or breaches across vendors and service providers.	Functional	Intersects With	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame as determined by the organization.
1.G	Supply Chain Incident Reporting	Organizations more rapidly learn about and respond to known incidents or breaches across vendors and service providers.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame as determined by the organization.
1.G	Supply Chain Incident Reporting	Organizations more rapidly learn about and respond to known incidents or breaches across vendors and service providers.	Functional	Intersects With	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected systems, applications and/or services that the organization utilizes.	5	Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame as determined by the organization.
1.H	Supply Chain Vulnerability Disclosure	Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.	Functional	Subset Of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization.
1.H	Supply Chain Vulnerability Disclosure	Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization.
1.H	Supply Chain Vulnerability Disclosure	Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.	Functional	Intersects With	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 systems, applications, services and data.	5	Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization.
1.H	Supply Chain Vulnerability Disclosure	Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.	Functional	Intersects With	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization.
1.H	Supply Chain Vulnerability Disclosure	Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.	Functional	Intersects With	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	5	Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization.
1.H	Supply Chain Vulnerability Disclosure	Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization.
1.H	Supply Chain Vulnerability Disclosure	Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization.
1.H	Supply Chain Vulnerability Disclosure	Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.	Functional	Intersects With	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization.
1.H	Supply Chain Vulnerability Disclosure	Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.	Functional	Intersects With	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization.
1.I	Vendor/Supplier Cybersecurity Requirements	Reduce risk by buying more secure products and services from more secure suppliers.	Functional	Intersects With	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	Organizations' procurement documents include cybersecurity requirements and questions, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.
1.I	Vendor/Supplier Cybersecurity Requirements	Reduce risk by buying more secure products and services from more secure suppliers.	Functional	Intersects With	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	Organizations' procurement documents include cybersecurity requirements and questions, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.
1.I	Vendor/Supplier Cybersecurity Requirements	Reduce risk by buying more secure products and services from more secure suppliers.	Functional	Intersects With	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	Organizations' procurement documents include cybersecurity requirements and questions, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.
1.I	Vendor/Supplier Cybersecurity Requirements	Reduce risk by buying more secure products and services from more secure suppliers.	Functional	Intersects With	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business information, systems and processes that are in scope by the third-party.	5	Organizations' procurement documents include cybersecurity requirements and questions, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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)
2.A	Changing Default Passwords	Prevent threat actors from using default passwords to achieve initial access or move laterally in a network.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting on any internal or external network. This includes IT assets for OT, such as OT administration web pages. In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices. OT: While changing default passwords on an organization's existing OT requires significantly more work, we still recommend having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversary TTPs change.
2.A	Changing Default Passwords	Prevent threat actors from using default passwords to achieve initial access or move laterally in a network.	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	An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting on any internal or external network. This includes IT assets for OT, such as OT administration web pages. In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices. OT: While changing default passwords on an organization's existing OT requires significantly more work, we still recommend having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversary TTPs change.
2.A	Changing Default Passwords	Prevent threat actors from using default passwords to achieve initial access or move laterally in a network.	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	An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting on any internal or external network. This includes IT assets for OT, such as OT administration web pages. In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices. OT: While changing default passwords on an organization's existing OT requires significantly more work, we still recommend having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversary TTPs change.
2.B	Minimum Password Strength	Organizational passwords are harder for threat actors to guess or crack.	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	Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected IT assets and all OT assets, when technically feasible.** Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement. This goal is particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks) or are unable to adopt passwordless authentication methods. * Modern attacker tools can crack eight-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember. ** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as those on offshore rigs or wind turbines.
2.B	Minimum Password Strength	Organizational passwords are harder for threat actors to guess or crack.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected IT assets and all OT assets, when technically feasible.** Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement. This goal is particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks) or are unable to adopt passwordless authentication methods. * Modern attacker tools can crack eight-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember. ** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as those on offshore rigs or wind turbines.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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)
2.B	Minimum Password Strength	Organizational passwords are harder for threat actors to guess or crack.	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	Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected IT assets and all OT assets, when technically feasible.** Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement. This goal is particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks) or are unable to adopt passwordless authentication methods. * Modern attacker tools can crack eight-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember. ** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as those on offshore rigs or wind turbines.
2.C	Unique Credentials	Attackers are unable to reuse compromised credentials to move laterally across the organization, particularly between IT and OT networks.	Functional	Equal	Unique Credentials	IAC-10.9	Mechanisms exist to implement security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems.	5	Organizations provision unique and separate credentials for similar services and asset access on IT and OT networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have passwords that are unique from all member user accounts.
2.D	Revoking Credentials for Departing Employees	Prevent unauthorized access to organizational accounts or resources by former employees.	Functional	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	A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.
2.D	Revoking Credentials for Departing Employees	Prevent unauthorized access to organizational accounts or resources by former employees.	Functional	Intersects With	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.
2.D	Revoking Credentials for Departing Employees	Prevent unauthorized access to organizational accounts or resources by former employees.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.
2.D	Revoking Credentials for Departing Employees	Prevent unauthorized access to organizational accounts or resources by former employees.	Functional	Intersects With	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	5	A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.
2.D	Revoking Credentials for Departing Employees	Prevent unauthorized access to organizational accounts or resources by former employees.	Functional	Intersects With	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.
2.E	Separating User and Privileged Accounts	Make it harder for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued need for a given set of permissions.
2.E	Separating User and Privileged Accounts	Make it harder for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.	Functional	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	No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued need for a given set of permissions.
2.E	Separating User and Privileged Accounts	Make it harder for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.	Functional	Intersects With	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	5	No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued need for a given set of permissions.
2.F	Network Segmentation	Reduce the likelihood of threat actors accessing the OT network after compromising the IT network.	Functional	Intersects With	Jump Server	AST-27	Mechanisms exist to conduct remote system administrative functions via a "jump box" or "jump server" that is located in a separate network zone to user workstations.	5	All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, “jump box,” or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.
2.F	Network Segmentation	Reduce the likelihood of threat actors accessing the OT network after compromising the IT network.	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	All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, “jump box,” or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.
2.F	Network Segmentation	Reduce the likelihood of threat actors accessing the OT network after compromising the IT network.	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	All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, “jump box,” or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.
2.F	Network Segmentation	Reduce the likelihood of threat actors accessing the OT network after compromising the IT network.	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	All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, “jump box,” or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.
2.G	Detection of Unsuccessful (Automated) Login Attempts	Protect organizations from automated, credential-based attacks.	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	All unsuccessful logins are logged and sent to an organization’s security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, a system-enforced policy prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10-minutes after 10 incorrect logins over a 10-minute period.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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)
2.G	Detection of Unsuccessful (Automated) Login Attempts	Protect organizations from automated, credential-based attacks.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, a system-enforced policy prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10-minutes after 10 incorrect logins over a 10-minute period.
2.G	Detection of Unsuccessful (Automated) Login Attempts	Protect organizations from automated, credential-based attacks.	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	All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, a system-enforced policy prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10-minutes after 10 incorrect logins over a 10-minute period.
2.G	Detection of Unsuccessful (Automated) Login Attempts	Protect organizations from automated, credential-based attacks.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, a system-enforced policy prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10-minutes after 10 incorrect logins over a 10-minute period.
2.G	Detection of Unsuccessful (Automated) Login Attempts	Protect organizations from automated, credential-based attacks.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, a system-enforced policy prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10-minutes after 10 incorrect logins over a 10-minute period.
2.H	Phishing-Resistant Multifactor Authentication (MFA)	Add a critical, additional layer of security to protect assets accounts whose credentials have been compromised.	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	Organizations implement MFA for access to assets using the strongest available method for that asset (see below for scope). MFA options sorted by strength, high to low, are as follows: 1. Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn or public key infrastructure (PKI) based - see CISA guidance in"Resources"); 2. If such hardware-based MFA is not available, then mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys are used; 3. MFA via short message service (SMS) or voice only used when no other options are possible. IT: All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems. OT: Within OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible HMIs.
2.H	Phishing-Resistant Multifactor Authentication (MFA)	Add a critical, additional layer of security to protect assets accounts whose credentials have been compromised.	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	Organizations implement MFA for access to assets using the strongest available method for that asset (see below for scope). MFA options sorted by strength, high to low, are as follows: 1. Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn or public key infrastructure (PKI) based - see CISA guidance in"Resources"); 2. If such hardware-based MFA is not available, then mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys are used; 3. MFA via short message service (SMS) or voice only used when no other options are possible. IT: All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems. OT: Within OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible HMIs.
2.I	Basic Cybersecurity Training	Organizational users learn and perform more secure behaviors.	Functional	Subset Of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness. New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.
2.I	Basic Cybersecurity Training	Organizational users learn and perform more secure behaviors.	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	At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness. New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.
2.I	Basic Cybersecurity Training	Organizational users learn and perform more secure behaviors.	Functional	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	At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness. New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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)
2.I	Basic Cybersecurity Training	Organizational users learn and perform more secure behaviors.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness. New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.
2.J	OT Cybersecurity Training	Personnel responsible for securing OT assets received specialized OT-focused cybersecurity training.	Functional	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	In addition to basic cybersecurity training, personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis.
2.J	OT Cybersecurity Training	Personnel responsible for securing OT assets received specialized OT-focused cybersecurity training.	Functional	Intersects With	Vendor Cybersecurity & Data Privacy Training	SAT-03.4	Mechanisms exist to incorporate vendor-specific security training in support of new technology initiatives.	5	In addition to basic cybersecurity training, personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis.
2.J	OT Cybersecurity Training	Personnel responsible for securing OT assets received specialized OT-focused cybersecurity training.	Functional	Intersects With	Privileged Users	SAT-03.5	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	5	In addition to basic cybersecurity training, personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis.
2.K	Strong and Agile Encryption	Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic.	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	Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithims, and consider managing implications of post-quantum cryptography. OT: To minimize the impact to latency and availability, encryption is used when feasible, usually for OT communications connecting with remote/external assets.
2.K	Strong and Agile Encryption	Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic.	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	Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithims, and consider managing implications of post-quantum cryptography. OT: To minimize the impact to latency and availability, encryption is used when feasible, usually for OT communications connecting with remote/external assets.
2.K	Strong and Agile Encryption	Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic.	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	Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithims, and consider managing implications of post-quantum cryptography. OT: To minimize the impact to latency and availability, encryption is used when feasible, usually for OT communications connecting with remote/external assets.
2.K	Strong and Agile Encryption	Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithims, and consider managing implications of post-quantum cryptography. OT: To minimize the impact to latency and availability, encryption is used when feasible, usually for OT communications connecting with remote/external assets.
2.K	Strong and Agile Encryption	Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic.	Functional	Intersects With	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithims, and consider managing implications of post-quantum cryptography. OT: To minimize the impact to latency and availability, encryption is used when feasible, usually for OT communications connecting with remote/external assets.
2.K	Strong and Agile Encryption	Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithims, and consider managing implications of post-quantum cryptography. OT: To minimize the impact to latency and availability, encryption is used when feasible, usually for OT communications connecting with remote/external assets.
2.K	Strong and Agile Encryption	Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic.	Functional	Intersects With	Technical Debt Reviews	SEA-02.3	Mechanisms exist to conduct ongoing “technical debt” reviews of hardware and software technologies to remediate outdated and/or unsupported technologies.	5	Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithims, and consider managing implications of post-quantum cryptography. OT: To minimize the impact to latency and availability, encryption is used when feasible, usually for OT communications connecting with remote/external assets.
2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.
2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.
2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	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	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.
2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	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	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.
2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.
2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.
2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	Functional	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	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.
2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	Functional	Intersects With	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.	5	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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)
2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	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	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.
2.L	Secure Sensitive Data	Protect sensitive information from unauthorized access.	Functional	Intersects With	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	5	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.
2.M	Email Security	Reduce risk from common email-based threats, such as spoofing, phishing, and interception.	Functional	Intersects With	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	On all corporate email infrastructure (1) STARTTLS is enabled, (2) Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are enabled, and (3) Domainbased Message Authentication, Reporting, and Conformance (DMARC) is enabled and set to "reject." For further examples and information, see CISA's past guidance for federal agencies.
2.M	Email Security	Reduce risk from common email-based threats, such as spoofing, phishing, and interception.	Functional	Intersects With	Sender Policy Framework (SPF)	NET-10.3	Mechanisms exist to validate the legitimacy of email communications through configuring a Domain Naming Service (DNS) Sender Policy Framework (SPF) record to specify the IP addresses and/or hostnames that are authorized to send email from the specified domain.	5	On all corporate email infrastructure (1) STARTTLS is enabled, (2) Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are enabled, and (3) Domainbased Message Authentication, Reporting, and Conformance (DMARC) is enabled and set to "reject." For further examples and information, see CISA's past guidance for federal agencies.
2.M	Email Security	Reduce risk from common email-based threats, such as spoofing, phishing, and interception.	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	On all corporate email infrastructure (1) STARTTLS is enabled, (2) Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are enabled, and (3) Domainbased Message Authentication, Reporting, and Conformance (DMARC) is enabled and set to "reject." For further examples and information, see CISA's past guidance for federal agencies.
2.N	Disable Macros by Default	Reduce the risk from embedded macros and similar executive code, a common and highly effective threat actor TTP.	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	A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.
2.N	Disable Macros by Default	Reduce the risk from embedded macros and similar executive code, a common and highly effective threat actor TTP.	Functional	Intersects With	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	5	A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.
2.O	Document Device Configurations	More efficiently and effectively manage, respond to, and recover from cyberattacks against the organization and maintain service continuity.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.
2.O	Document Device Configurations	More efficiently and effectively manage, respond to, and recover from cyberattacks against the organization and maintain service continuity.	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	Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.
2.O	Document Device Configurations	More efficiently and effectively manage, respond to, and recover from cyberattacks against the organization and maintain service continuity.	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	Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.
2.O	Document Device Configurations	More efficiently and effectively manage, respond to, and recover from cyberattacks against the organization and maintain service continuity.	Functional	Intersects With	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	5	Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.
2.P	Document Network Topology	More efficiently and effectively respond to cyberattacks and maintain service continuity.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and OT networks. Periodic reviews and updates should be performed and tracked on a recurring basis.
2.P	Document Network Topology	More efficiently and effectively respond to cyberattacks and maintain service continuity.	Functional	Intersects With	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for systems, applications, services and third parties by graphically representing applicable boundaries.	5	Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and OT networks. Periodic reviews and updates should be performed and tracked on a recurring basis.
2.Q	Hardware and Software Approval Process	Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.	Functional	Subset Of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.
2.Q	Hardware and Software Approval Process	Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.	Functional	Intersects With	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.
2.Q	Hardware and Software Approval Process	Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.	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	Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.
2.Q	Hardware and Software Approval Process	Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.
2.Q	Hardware and Software Approval Process	Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.
2.Q	Hardware and Software Approval Process	Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.
2.Q	Hardware and Software Approval Process	Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity & data privacy controls.	5	Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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)
2.Q	Hardware and Software Approval Process	Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.	Functional	Intersects With	Security Authorization	IAO-07	Mechanisms exist to ensure systems, projects and services are officially authorized prior to "go live" in a production environment.	5	Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.
2.R	System Backups	Organizations reduce the likelihood and duration of data loss at loss of service delivery or operations.	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	All systems that are necessary for operations are regularly backed up on a regular cadence (no less than once per year). Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for OT assets includes at a minimum: configurations, roles, programmable controller (PLC) logic, engineering drawings, and tools.
2.R	System Backups	Organizations reduce the likelihood and duration of data loss at loss of service delivery or operations.	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	All systems that are necessary for operations are regularly backed up on a regular cadence (no less than once per year). Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for OT assets includes at a minimum: configurations, roles, programmable controller (PLC) logic, engineering drawings, and tools.
2.R	System Backups	Organizations reduce the likelihood and duration of data loss at loss of service delivery or operations.	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	All systems that are necessary for operations are regularly backed up on a regular cadence (no less than once per year). Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for OT assets includes at a minimum: configurations, roles, programmable controller (PLC) logic, engineering drawings, and tools.
2.S	Incident Response (IR) Plans	Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.	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	Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as feasible. IR plans are drilled at least annually, and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.
2.S	Incident Response (IR) Plans	Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.	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	Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as feasible. IR plans are drilled at least annually, and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.
2.S	Incident Response (IR) Plans	Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.	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	Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as feasible. IR plans are drilled at least annually, and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.
2.S	Incident Response (IR) Plans	Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.	Functional	Intersects With	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as feasible. IR plans are drilled at least annually, and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.
2.S	Incident Response (IR) Plans	Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.	Functional	Intersects With	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to: (1) Determine the effectiveness of incident response processes; (2) Continuously improve incident response processes; and (3) Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.	5	Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as feasible. IR plans are drilled at least annually, and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.
2.S	Incident Response (IR) Plans	Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.	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	Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as feasible. IR plans are drilled at least annually, and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.
2.T	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
2.T	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks.	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	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
2.T	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks.	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
2.T	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks.	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	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
2.T	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks.	Functional	Intersects With	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
2.T	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks.	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	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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)
2.T	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks.	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	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
2.T	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks.	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	5	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
2.T	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks.	Functional	Intersects With	Integration of Scanning & Other Monitoring Information	MON-02.3	Automated mechanisms exist to integrate the analysis of audit records with analysis of vulnerability scanners, network performance, system monitoring and other sources to further enhance the ability to identify inappropriate or unusual activity.	5	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
2.T	Log Collection	Achieve better visibility to detect and effectively respond to cyberattacks.	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	Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.
2.U	Secure Log Storage	Organizations' security logs are protected from unauthorized access and tampering.	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	Logs are stored in a central system, such as a security information and event management tool or central database, and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.
2.U	Secure Log Storage	Organizations' security logs are protected from unauthorized access and tampering.	Functional	Intersects With	Event Log Backup on Separate Physical Systems / Components	MON-08.1	Mechanisms exist to back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool.	5	Logs are stored in a central system, such as a security information and event management tool or central database, and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.
2.U	Secure Log Storage	Organizations' security logs are protected from unauthorized access and tampering.	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	Logs are stored in a central system, such as a security information and event management tool or central database, and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.
2.U	Secure Log Storage	Organizations' security logs are protected from unauthorized access and tampering.	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	Logs are stored in a central system, such as a security information and event management tool or central database, and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.
2.V	Prohibit Connection of Unauthorized Devices	Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices.	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	Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun. OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices or establish procedures for granting access through approved exceptions.
2.V	Prohibit Connection of Unauthorized Devices	Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun. OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices or establish procedures for granting access through approved exceptions.
2.V	Prohibit Connection of Unauthorized Devices	Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices.	Functional	Intersects With	Interface Security	EMB-04	Mechanisms exist to protect embedded devices against unauthorized use of the physical factory diagnostic and test interface(s).	5	Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling AutoRun. OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices or establish procedures for granting access through approved exceptions.
2.W	No Exploitable Services on the Internet	Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in public-facing assets.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	Assets on the public internet expose no exploitable services, such as remote desktop protocol. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets.
2.W	No Exploitable Services on the Internet	Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in public-facing assets.	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	Assets on the public internet expose no exploitable services, such as remote desktop protocol. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets.
2.W	No Exploitable Services on the Internet	Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in public-facing assets.	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	Assets on the public internet expose no exploitable services, such as remote desktop protocol. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets.
2.W	No Exploitable Services on the Internet	Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in public-facing assets.	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	Assets on the public internet expose no exploitable services, such as remote desktop protocol. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets.
2.X	Limit OT Connections to Public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet.	Functional	Intersects With	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).
2.X	Limit OT Connections to Public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet.	Functional	Intersects With	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).
2.X	Limit OT Connections to Public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet.	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	No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)

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)
2.X	Limit OT Connections to Public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet.	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	No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).
2.X	Limit OT Connections to Public Internet	Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet.	Functional	Intersects With	Direct Internet Access Restrictions	NET-06.5	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive / regulated data enclaves (secure zones).	5	No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).
3.A	Detecting Relevant Threats and TTPs	Organizations are aware of and able to detect relevant threats and TTPs.	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5	Organizations document a list of threats and cyber actor TTPs relevant to their organization (e.g., based on industry, sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.
3.A	Detecting Relevant Threats and TTPs	Organizations are aware of and able to detect relevant threats and TTPs.	Functional	Subset Of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	Organizations document a list of threats and cyber actor TTPs relevant to their organization (e.g., based on industry, sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.
3.A	Detecting Relevant Threats and TTPs	Organizations are aware of and able to detect relevant threats and TTPs.	Functional	Intersects With	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	Organizations document a list of threats and cyber actor TTPs relevant to their organization (e.g., based on industry, sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.
3.A	Detecting Relevant Threats and TTPs	Organizations are aware of and able to detect relevant threats and TTPs.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	Organizations document a list of threats and cyber actor TTPs relevant to their organization (e.g., based on industry, sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.
3.A	Detecting Relevant Threats and TTPs	Organizations are aware of and able to detect relevant threats and TTPs.	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	Organizations document a list of threats and cyber actor TTPs relevant to their organization (e.g., based on industry, sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.
4.A	Incident Reporting	CISA and other organizations are better able to provide assistance or understand the broader scope of a cyberattack.	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	Organizations maintain codified policy and procedures on to whom and how to report all confirmed cybersecurity incidents to appropriate external entities (e.g., state/federal regulators or SRMA's as required, ISAC/ISAO, as well as CISA). Known incidents are reported to CISA as well as other necessary parties within time frames directed by applicable regulatory guidance or in the absence of guidance, as soon as safely capable. This goal will be revisited following full implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).
4.A	Incident Reporting	CISA and other organizations are better able to provide assistance or understand the broader scope of a cyberattack.	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	Organizations maintain codified policy and procedures on to whom and how to report all confirmed cybersecurity incidents to appropriate external entities (e.g., state/federal regulators or SRMA's as required, ISAC/ISAO, as well as CISA). Known incidents are reported to CISA as well as other necessary parties within time frames directed by applicable regulatory guidance or in the absence of guidance, as soon as safely capable. This goal will be revisited following full implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).
4.B	Vulnerability Disclosure/Reporting	Organizations more rapidly learn about vulnerabilities or weaknesses in their assets discovered by security researchers; researchers are more incentivized to responsibly share their findings.	Functional	Intersects With	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of products and services that receives unsolicited input from the public about vulnerabilities in organizational systems, services and processes.	5	Consistent with NIST SP 800-53 Revision 5, organizations maintain a public, easily discoverable method for security researchers to notify (e.g., via email address or web form) organizations' security teams of vulnerable, misconfigured, or otherwise exploitable assets. Valid submissions are acknowledged and responded to in a timely manner, taking into account the completeness and complexity of the vulnerability. Validated and exploitable weaknesses are mitigated consistent with their severity. Security researchers sharing vulnerabilities discovered in good faith are protected under Safe Harbor rules. In instances where vulnerabilities are validated and disclosed, public acknowledgement is given to the researcher who originally submitted the notification.
4.B	Vulnerability Disclosure/Reporting	Organizations more rapidly learn about vulnerabilities or weaknesses in their assets discovered by security researchers; researchers are more incentivized to responsibly share their findings.	Functional	Intersects With	Security Disclosure Contact Information	THR-06.1	Mechanisms exist to enable security researchers to submit discovered vulnerabilities.	5	Consistent with NIST SP 800-53 Revision 5, organizations maintain a public, easily discoverable method for security researchers to notify (e.g., via email address or web form) organizations' security teams of vulnerable, misconfigured, or otherwise exploitable assets. Valid submissions are acknowledged and responded to in a timely manner, taking into account the completeness and complexity of the vulnerability. Validated and exploitable weaknesses are mitigated consistent with their severity. Security researchers sharing vulnerabilities discovered in good faith are protected under Safe Harbor rules. In instances where vulnerabilities are validated and disclosed, public acknowledgement is given to the researcher who originally submitted the notification.
4.C	Deploy Security.TXT Files	Allow security researchers to submit discovered weaknesses or vulnerabilities faster.	Functional	Equal	Security Disclosure Contact Information	THR-06.1	Mechanisms exist to enable security researchers to submit discovered vulnerabilities.	10	All public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116.
5.A	Incident Planning and Preparedness	Organizations are capable of safely and effectively recovering from a cybersecurity incident.	Functional	Subset Of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.
5.A	Incident Planning and Preparedness	Organizations are capable of safely and effectively recovering from a cybersecurity incident.	Functional	Intersects With	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.
5.A	Incident Planning and Preparedness	Organizations are capable of safely and effectively recovering from a cybersecurity incident.	Functional	Intersects With	Continue Essential Mission & Business Functions	BCD-02.2	Mechanisms exist to continue essential missions and business functions with little or no loss of operational continuity and sustain that continuity until full system restoration at primary processing and/or storage sites.	5	Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.
5.A	Incident Planning and Preparedness	Organizations are capable of safely and effectively recovering from a cybersecurity incident.	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	Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.
5.A	Incident Planning and Preparedness	Organizations are capable of safely and effectively recovering from a cybersecurity incident.	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	Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)