#	SCF Domain	SCF Identifier	Security & Privacy by Design (S|P) Principles	Principle Intent
1	Security & Privacy Governance	GOV	Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity and privacy principles that address applicable statutory, regulatory and contractual obligations.	Organizations specify the development of an organization's cybersecurity and privacy programs, including criteria to measure success, to ensure ongoing leadership engagement and risk management.
2	Artificial and Autonomous Technology	AAT	Ensure trustworthy and resilient Artificial Intelligence (AI) and autonomous technologies to achieve a beneficial impact by informing, advising or simplifying tasks, while minimizing emergent properties or unintended consequences.	Organizations ensure Artificial Intelligence (AI) and autonomous technologies are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and privacy-enhanced. In addition, AI-related risks are governed according to technology-specific considerations to minimize emergent properties or unintended consequences.
3	Asset Management	AST	Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.	Organizations ensure technology assets are properly managed throughout the lifecycle of the asset, from procurement through disposal, ensuring only authorized devices are allowed to access the organization's network and to protect the organization's data that is stored, processed or transmitted on its assets.
4	Business Continuity & Disaster Recovery	BCD	Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.	Organizations establish processes that will help the organization recover from adverse situations with minimal impact to operations, as well as provide the capability for e-discovery.
5	Capacity & Performance Planning	CAP	Govern the current and future capacities and performance of technology assets.	Organizations prevent avoidable business interruptions caused by capacity and performance limitations by proactively planning for growth and forecasting, as well as requiring both technology and business leadership to maintain situational awareness of current and future performance.
6	Change Management	CHG	Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.	Organizations ensure both technology and business leadership proactively manage change, including the assessment, authorization and monitoring of technical changes across the enterprise so as to not impact production systems uptime and allow easier troubleshooting of issues.
7	Cloud Security	CLD	Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal cybersecurity and privacy controls.	Organizations govern the use of private and public cloud environments (e.g., IaaS, PaaS and SaaS) to holistically manage risks associated with third-party involvement and architectural decisions, as well as to ensure the portability of data to change cloud providers, if needed.
8	Compliance	CPL	Oversee the execution of cybersecurity and privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.	Organizations ensure controls are in place to ensure adherence to applicable statutory, regulatory and contractual compliance obligations, as well as internal company standards.
9	Configuration Management	CFG	Enforce secure configurations for systems, applications and services according to vendor-recommended and industry-recognized secure practices.	Organizations establish and maintain the integrity of systems. Without properly documented and implemented configuration management controls, security features can be inadvertently or deliberately omitted or rendered inoperable, allowing processing irregularities to occur or the execution of malicious code.
10	Continuous Monitoring	MON	Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.	Organizations establish and maintain ongoing situational awareness across the enterprise through the centralized collection and review of security-related event logs. Without comprehensive visibility into infrastructure, operating system, database, application and other logs, the organization will have "blind spots" in its situational awareness that could lead to system compromise, data exfiltration, or unavailability of needed computing resources.
11	Cryptographic Protections	CRY	Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulated data both at rest and in transit.	Organizations ensure the confidentiality and integrity of its data through implementing appropriate cryptographic technologies to protect systems, applications, services and data.
12	Data Classification & Handling	DCH	Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.	Organizations ensure that technology assets, both electronic and physical, are properly classified and measures implemented to protect the organization's data from unauthorized disclosure, or modification, regardless if it is being transmitted or stored. Applicable statutory, regulatory and contractual compliance requirements dictate the minimum safeguards that must be in place to protect the confidentiality, integrity and availability of data.
13	Embedded Technology	EMB	Provide additional scrutiny to reduce the risks associated with embedded technology, based on the potential damages posed from malicious use of the technology.	Organizations specify the development, proactive management and ongoing review of security embedded technologies, including hardening of the "stack" from the hardware, firmware and software to transmission and service protocols used for Internet of Things (IoT) and Operational Technology (OT) devices.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

#	SCF Domain	SCF Identifier	Security & Privacy by Design (S|P) Principles	Principle Intent
14	Endpoint Security	END	Harden endpoint devices to protect against reasonable threats to those devices and the data those devices store, transmit and process.	Organizations ensure that endpoint devices are appropriately protected from security threats to the device and its data. Applicable statutory, regulatory and contractual compliance requirements dictate the minimum safeguards that must be in place to protect the confidentiality, integrity, availability and safety considerations.
15	Human Resources Security	HRS	Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity and privacy-minded workforce.	Organizations create a cybersecurity and privacy-minded workforce and an environment that is conducive to innovation, considering issues such as culture, reward and collaboration.
16	Identification & Authentication	IAC	Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.	Organizations implement the concept of "least privilege" through limiting access to the organization's systems and data to authorized users only.
17	Incident Response	IRO	Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).	Organizations establish and maintain a viable and tested capability to respond to cybersecurity or privacy-related incidents in a timely manner, where organizational personnel understand how to detect and report potential incidents.
18	Information Assurance	IAO	Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity and privacy controls, prior to a system, application or service being used in a production environment.	Organizations ensure the adequately of cybersecurity and privacy controls in development, testing and production environments.
19	Maintenance	MNT	Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.	Organizations ensure that technology assets are properly maintained to ensure continued performance and effectiveness. Maintenance processes apply additional scrutiny to the security of end-of-life or unsupported assets.
20	Mobile Device Management	MDM	Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulated data that limit the attack surface and potential data exposure from mobile device usage.	Organizations govern risks associated with mobile devices, regardless of ownership (organization-owned, employee-owned or third-party owned). Wherever possible, technologies are employed to centrally manage mobile device access and data storage practices.
21	Network Security	NET	Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.	Organizations ensure sufficient cybersecurity and privacy controls are architected to protect the confidentiality, integrity, availability and safety of the organization's network infrastructure, as well as to provide situational awareness of activity on the organization's networks.
22	Physical & Environmental Security	PES	Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.	Organizations minimize physical access to the organization's systems and data by addressing applicable physical security controls and ensuring that appropriate environmental controls are in place and continuously monitored to ensure equipment does not fail due to environmental threats.
23	Privacy	PRI	Align privacy practices with industry-recognized privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.	Organizations align privacy engineering decisions with the organization's overall privacy strategy and industry-recognized leading practices to secure Personal Data (PD) that implements the concept of privacy by design and by default.
24	Project & Resource Management	PRM	Operationalize a viable strategy to achieve cybersecurity & privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.	Organizations ensure that security-related projects have both resource and project/program management support to ensure successful project execution.
25	Risk Management	RSK	Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.	Organizations ensure that the business unit(s) that own the assets and / or processes involved are made aware of and understand all applicable cybersecurity and privacy-related risks. The cybersecurity and privacy teams advise and educate on risk management matters, while it is the business units and other key stakeholders that ultimately own the risk.
26	Secure Engineering & Architecture	SEA	Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.	Organizations align cybersecurity engineering and architecture decisions with the organization's overall technology architectural strategy and industry-recognized leading practices to secure networked environments.
27	Security Operations	OPS	Execute the delivery of cybersecurity and privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.	Organizations ensure appropriate resources and a management structure exists to enable the service delivery of cybersecurity, physical security and privacy operations.
28	Security Awareness & Training	SAT	Foster a cybersecurity and privacy-minded workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.	Organizations develop a cybersecurity and privacy-minded workforce through continuous education activities and practical exercises.
29	Technology Development & Acquisition	TDA	Develop and test systems, applications or services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design weaknesses.	Organizations ensure that cybersecurity and privacy principles are implemented into any products/solutions, either developed internally or acquired, to make sure that the concepts of "least privilege" and "least functionality" are incorporated.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

#	SCF Domain	SCF Identifier	Security & Privacy by Design (S|P) Principles	Principle Intent
30	Third-Party Management	TPM	Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.	Organizations ensure that cybersecurity and privacy risks associated with third-parties are minimized and enable measures to sustain operations should a third-party become compromised, untrustworthy or defunct.
31	Threat Management	THR	Proactively identify and assess technology-related threats, to both assets and business processes, to determine the applicable risk and necessary corrective action.	Organizations establish a capability to proactively identify and manage technology-related threats to the cybersecurity and privacy of the organization's systems, data and business processes.
32	Vulnerability & Patch Management	VPM	Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.	Organizations proactively manage the risks associated with technical vulnerability management that includes ensuring good patch and change management practices are utilized.
33	Web Security	WEB	Ensure the security and resilience of Internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.	Organizations address the risks associated with Internet-accessible technologies by hardening devices, monitoring system file integrity, enabling auditing, and monitoring for malicious activities.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Methods To Comply With SCF Controls	Evidence Request List (ERL) #	SCF Control Question	Relative Control Weighting
Cybersecurity & Privacy Governance	Digital Security Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and privacy governance controls.	- Steering committee - Digital Security Program (DSP) - Cybersecurity & Data Protection Program (CDPP)	E-GOV-01 E-GOV-02	Does the organization staff a function to centrally-govern cybersecurity and privacy controls?	10
Cybersecurity & Privacy Governance	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprised of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.	- Steering committee - Digital Security Program (DSP) - Cybersecurity & Data Protection Program (CDPP)	E-GOV-03	Does the organization coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprised of key cybersecurity, privacy and business executives, which meets formally and on a regular basis?	7
Cybersecurity & Privacy Governance	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and privacy program.		E-CPL-05 E-CPL-09 E-GOV-03 E-GOV-04 E-GOV-05 E-GOV-06	Does the organization provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and privacy program?	5
Cybersecurity & Privacy Governance	Publishing Cybersecurity & Privacy Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.	- Steering committee - Digital Security Program (DSP) - Cybersecurity & Data Protection Program (CDPP) - Governance, Risk and Compliance Solution (GRC) tool (SCFConnect, SureCloud,Ostendio, ZenGRC, Archer, RSAM,	E-GOV-08 E-GOV-09 E-GOV-11	Does the organization establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures?	10
Cybersecurity & Privacy Governance	Periodic Review & Update of Cybersecurity & Privacy Program	GOV-03	Mechanisms exist to review the cybersecurity and privacy program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	- Governance, Risk and Compliance Solution (GRC) tool (SCFConnect, SureCloud,Ostendio, ZenGRC, Archer, RSAM, MetricStream, etc.) - Steering committee	E-GOV-12	Does the organization review cybersecurity and privacy policies, standards and procedures at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness?	7
Cybersecurity & Privacy Governance	Assigned Cybersecurity & Privacy Responsibilities	GOV-04	Mechanisms exist to assign a qualified individual with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program.	- NIST NICE Framework - Chief Information Security Officer (CISO)	E-HRS-01 E-HRS-05 E-HRS-06 E-HRS-07 E-HRS-08 E-HRS-09	Does the organization assign a qualified individual with the mission and resources to centrally-manage coordinate, develop, implement and maintain an enterprise-wide cybersecurity and privacy program?	10
Cybersecurity & Privacy Governance	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.	- Documented roles and responsibilities	E-HRS-15	Does the organization 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?	8
Cybersecurity & Privacy Governance	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.	- Organization chart	E-HRS-15	Does the organization 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?	7
Cybersecurity & Privacy Governance	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and privacy program measures of performance.	- Metrics - Governance, Risk and Compliance Solution (GRC) tool (SCFConnect, SureCloud,Ostendio, ZenGRC, Archer, RSAM, MetricStream, etc.) - Enterprise Risk Management (ERM) solution	E-GOV-13	Does the organization develop, report and monitor cybersecurity and privacy program measures of performance?	6
Cybersecurity & Privacy Governance	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the cybersecurity and privacy program.	- Key Performance Indicators (KPIs)		Does the organization develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the cybersecurity and privacy program?	6
Cybersecurity & Privacy Governance	Key Risk Indicators (KRIs)	GOV-05.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the cybersecurity and privacy program.	- Key Risk Indicators (KRIs)		Does the organization develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the cybersecurity and privacy program?	6
Cybersecurity & Privacy Governance	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	- Threat intelligence personnel - Integrated Security Incident Response Team (ISIRT)		Does the organization identify and document appropriate contacts within relevant law enforcement and regulatory bodies?	5

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Cybersecurity & Privacy Governance	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & privacy communities to: • Facilitate ongoing cybersecurity and privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity and privacy practices, techniques and technologies; and	- SANS - CISO Executive Network - ISACA chapters - IAPP chapters - ISAA chapters	E-THR-02	Does the organization establish contact with selected groups and associations within the cybersecurity & privacy communities to: • Facilitate ongoing cybersecurity and privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity and privacy practices,	7
Cybersecurity & Privacy Governance	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the mission of the organization.		E-PRM-01	Does the organization define the context of its business model and document the mission of the organization?	5
Cybersecurity & Privacy Governance	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.		E-GOV-10	Does the organization establish control objectives as the basis for the selection, implementation and management of the organization's internal control system?	5
Cybersecurity & Privacy Governance	Data Governance	GOV-10	Mechanisms exist to facilitate data governance to oversee the organization's policies, standards and procedures so that sensitive/regulated data is effectively managed and maintained in accordance with applicable statutory, regulatory and contractual obligations.			Does the organization establish data governance across the organization?	9
Cybersecurity & Privacy Governance	Purpose Validation	GOV-11	Mechanisms exist to monitor mission/business-critical services or functions to ensure those resources are being used consistent with their intended purpose.			Does the organization analyze supporting mission essential services or functions to ensure those resources are being used consistent with their intended purpose?	5
Cybersecurity & Privacy Governance	Forced Technology Transfer (FTT)	GOV-12	Mechanisms exist to avoid and/or constrain the forced exfiltration of sensitive / regulated information (e.g., Intellectual Property (IP)) to the host government for purposes of market access or market management practices.	- Board of Directors (Bod) Ethics Committee		Does the organization avoid and/or constrain the forced exfiltration of sensitive / regulated information (e.g., Intellectual Property (IP)) to the host government for purposes of market access or market management practices?	10
Cybersecurity & Privacy Governance	State-Sponsored Espionage	GOV-13	Mechanisms exist to constrain the host government's ability to leverage the organization's technology assets for economic or political espionage and/or cyberwarfare activities.	- Board of Directors (Bod) Ethics Committee		Does the organization constrain the host government's ability to leverage the organization's technology assets for economic or political espionage and/or cyberwarfare activities?	10
Cybersecurity & Privacy Governance	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity and privacy principles into Business As Usual (BAU) practices through executive leadership involvement.			Does the organization incorporate cybersecurity and privacy principles into Business As Usual (BAU) practices through executive leadership involvement?	6
Cybersecurity & Privacy Governance	Operationalizing Cybersecurity & Privacy Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and privacy practices for each system, application and/or service under their control.			Does the organization compel data and/or process owners to operationalize cybersecurity and privacy practices for each system, application and/or service under their control?	9
Cybersecurity & Privacy Governance	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity and privacy controls for each system, application and/or service under their control.			Does the organization compel data and/or process owners to select required cybersecurity and privacy controls for each system, application and/or service under their control?	8
Cybersecurity & Privacy Governance	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity and privacy controls for each system, application and/or service under their control.			Does the organization compel data and/or process owners to implement required cybersecurity and privacy controls for each system, application and/or service under their control?	9
Cybersecurity & Privacy Governance	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity and privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.			Does the organization compel data and/or process owners to assess if required cybersecurity and privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended?	8
Cybersecurity & Privacy Governance	Authorize Systems, Applications & Services	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.			Does the organization compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Cybersecurity & Privacy Governance	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity and privacy controls are operating as intended.			Does the organization compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity and privacy controls are operating as intended?	8
Artificial & Autonomous Technologies	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.			Does the organization ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively?	10
Artificial & Autonomous Technologies	AI & Autonomous Technologies-Related Legal Requirements Definition	AAT-01.1	Mechanisms exist to identify, understand, document and manage applicable statutory and regulatory requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization identify, understand, document and manage applicable statutory and regulatory requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT)	8
Artificial & Autonomous Technologies	Trustworthy AI & Autonomous Technologies	AAT-01.2	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and privacy-enhanced to minimize emergent properties or unintended consequences.			Does the organization ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and privacy-enhanced to minimize emergent properties or unintended consequences?	10
Artificial & Autonomous Technologies	AI & Autonomous Technologies Value Sustainment	AAT-01.3	Mechanisms exist to sustain the value of deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization sustain the value of deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT)	1
Artificial & Autonomous Technologies	Situational Awareness of AI & Autonomous Technologies	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).			Does the organization develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party)?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Risk Mapping	AAT-02.1	Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies (AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements.			Does the organization identify Artificial Intelligence (AI) and Autonomous Technologies (AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Internal Controls	AAT-02.2	Mechanisms exist to identify and document internal cybersecurity and privacy controls for Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization identify and document internal cybersecurity and privacy controls for Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Context Definition	AAT-03	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: • Intended purposes; • Potentially beneficial uses; • Context-specific laws and regulations;			Does the organization establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: • Intended purposes; • Potentially beneficial uses; • Context-specific laws and regulations;	8
Artificial & Autonomous Technologies	AI & Autonomous Technologies Mission and Goals Definition	AAT-03.1	Mechanisms exist to define and document the organization's mission and defined goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization define and document the organization's mission and defined goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	8
Artificial & Autonomous Technologies	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT)	8
Artificial & Autonomous Technologies	AI & Autonomous Technologies Potential Benefits Analysis	AAT-04.1	Mechanisms exist to assess the potential benefits of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization assess the potential benefits of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	2
Artificial & Autonomous Technologies	AI & Autonomous Technologies Potential Costs Analysis	AAT-04.2	Mechanisms exist to assess potential costs, including non-monetary costs, resulting from expected or realized Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related errors or system functionality and trustworthiness.			Does the organization assess potential costs, including non-monetary costs, resulting from expected or realized Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related errors or system functionality and trustworthiness?	2

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Artificial & Autonomous Technologies	AI & Autonomous Technologies Targeted Application Scope	AAT-04.3	Mechanisms exist to specify and document the targeted application scope of the proposed use and operation of Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization specify and document the targeted application scope of the proposed use and operation of Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	8
Artificial & Autonomous Technologies	AI & Autonomous Technologies Cost / Benefit Mapping	AAT-04.4	Mechanisms exist to map risks and benefits for all components of Artificial Intelligence (AI) and Autonomous Technologies (AAT), including third-party software and data.			Does the organization map risks and benefits for all components of Artificial Intelligence (AI) and Autonomous Technologies (AAT), including third-party software and data?	2
Artificial & Autonomous Technologies	AI & Autonomous Technologies Training	AAT-05	Mechanisms exist to ensure personnel and external stakeholders are provided with position-specific risk management training for Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization ensure personnel and external stakeholders are provided with position-specific risk management training for Artificial Intelligence (AI) and Autonomous Technologies (AAT)	5
Artificial & Autonomous Technologies	AI & Autonomous Technologies Fairness & Bias	AAT-06	Mechanisms exist to prevent Artificial Intelligence (AI) and Autonomous Technologies (AAT) from unfairly identifying, profiling and/or statistically singling out a segmented population defined by race, religion, gender identity, national origin, religion, disability or any other politically-charged identifier.			Does the organization prevent Artificial Intelligence (AI) and Autonomous Technologies (AAT) from unfairly identifying, profiling and/or statistically singling out a segmented population defined by race, religion, gender identity, national origin, religion, disability or any other politically-charged identifier?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.			Does the organization leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks?	10
Artificial & Autonomous Technologies	AI & Autonomous Technologies Impact Characterization	AAT-07.1	Mechanisms exist to characterize the impacts of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society.			Does the organization characterize the impacts of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society?	8
Artificial & Autonomous Technologies	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.			Does the organization define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts?	10
Artificial & Autonomous Technologies	AI & Autonomous Technologies Continuous Improvements	AAT-07.3	Mechanisms exist to continuously improve Artificial Intelligence (AI) and Autonomous Technologies (AAT) capabilities to maximize benefits and minimize negative impacts associated with AAT.			Does the organization continuously improve Artificial Intelligence (AI) and Autonomous Technologies (AAT) capabilities to maximize benefits and minimize negative impacts associated with AAT?	8
Artificial & Autonomous Technologies	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.			Does the organization define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Risk Profiling	AAT-09	Mechanisms exist to document the risks and potential impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT) designed, developed, deployed, evaluated and used.			Does the organization document the risks and potential impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT) designed, developed, deployed, evaluated and used?	9
Artificial & Autonomous Technologies	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related testing, identification of incidents and information sharing.		E-IAO-02	Does the organization implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related testing, identification of incidents and information sharing?	10
Artificial & Autonomous Technologies	AI TEVV Trustworthiness Assessment	AAT-10.1	Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy behavior and operation including security, anonymization and disaggregation of captured and stored data for approved purposes.			Does the organization evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy behavior and operation including security, anonymization and disaggregation of captured and stored data for approved purposes?	10
Artificial & Autonomous Technologies	AI TEVV Tools	AAT-10.2	Mechanisms exist to document test sets, metrics and details about the tools used during Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices.			Does the organization document test sets, metrics and details about the tools used during AI TEVV?	7

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Artificial & Autonomous Technologies	AI TEVV Trustworthiness Demonstration	AAT-10.3	Mechanisms exist to demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed is valid, reliable and operate as intended based on approved designs.			Does the organization demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed is valid, reliable and operate as intended based on approved designs.?	9
Artificial & Autonomous Technologies	AI TEVV Safety Demonstration	AAT-10.4	Mechanisms exist to demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed are safe, residual risk does not exceed the organization's risk tolerance and can fail safely, particularly if made to operate beyond its knowledge limits.			Does the organization demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed are safe, residual risk does not exceed the organization's risk tolerance and can fail safely, particularly if made to operate beyond its knowledge limits?	10
Artificial & Autonomous Technologies	AI TEVV Resiliency Assessment	AAT-10.5	Mechanisms exist to evaluate the security and resilience of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.			Does the organization evaluate the security and resilience of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed?	6
Artificial & Autonomous Technologies	AI TEVV Transparency & Accountability Assessment	AAT-10.6	Mechanisms exist to examine risks associated with transparency and accountability of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.			Does the organization examine risks associated with transparency and accountability of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed?	7
Artificial & Autonomous Technologies	AI TEVV Privacy Assessment	AAT-10.7	Mechanisms exist to examine the privacy risk of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.			Does the organization examine the privacy risk of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed?	9
Artificial & Autonomous Technologies	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.			Does the organization examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Model Validation	AAT-10.9	Mechanisms exist to validate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) model.			Does the organization validate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) model?	5
Artificial & Autonomous Technologies	AI TEVV Results Evaluation	AAT-10.10	Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) to determine the viability of the proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization evaluate the results of AI TEVV to determine the viability of the proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	10
Artificial & Autonomous Technologies	AI TEVV Effectiveness	AAT-10.11	Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV).			Does the organization evaluate the effectiveness of the processes utilized to perform AI TEVV?	5
Artificial & Autonomous Technologies	AI TEVV Comparable Deployment Settings	AAT-10.12	Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related performance or the assurance criteria demonstrated for conditions similar to deployment settings.			Does the organization evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related performance or the assurance criteria demonstrated for conditions similar to deployment settings?	5
Artificial & Autonomous Technologies	AI TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization proactively monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	9
Artificial & Autonomous Technologies	Updating AI & Autonomous Technologies	AAT-10.14	Mechanisms exist to integrate continual improvements for deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization integrate continual improvements for deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	9
Artificial & Autonomous Technologies	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.			Does the organization compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Artificial & Autonomous Technologies	AI & Autonomous Technologies Stakeholder Feedback Integration	AAT-11.1	Mechanisms exist to regularly collect, consider, prioritize and integrate risk-related feedback from those external to the team that developed or deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization regularly collect, consider, prioritize and integrate risk-related feedback from those external to the team that developed or deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.			Does the organization conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies End User Feedback	AAT-11.3	Mechanisms exist to collect and integrate feedback from end users and impacted communities into Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related system evaluation metrics.			Does the organization collect and integrate feedback from end users and impacted communities into Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related system evaluation metrics?	7
Artificial & Autonomous Technologies	AI & Autonomous Technologies Incident & Error Reporting	AAT-11.4	Mechanisms exist to communicate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related incidents and/or errors to relevant stakeholders, including affected communities.			Does the organization communicate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related incidents and/or errors to relevant stakeholders, including affected communities?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to identify data sources for Artificial Intelligence (AI) and Autonomous Technologies (AAT) to prevent third-party Intellectual Property (IP) rights infringement.			Does the organization identify data sources for Artificial Intelligence (AI) and Autonomous Technologies (AAT) to prevent third-party Intellectual Property (IP) rights infringement?	10
Artificial & Autonomous Technologies	AI & Autonomous Technologies Stakeholder Diversity	AAT-13	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholder competencies, skills and capacities incorporate demographic diversity, broad domain and user experience expertise.			Does the organization ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholder competencies, skills and capacities incorporate demographic diversity, broad domain and user experience expertise?	8
Artificial & Autonomous Technologies	AI & Autonomous Technologies Stakeholder Competencies	AAT-13.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related operator and practitioner proficiency requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT) are defined, assessed and documented.			Does the organization ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related operator and practitioner proficiency requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT) are defined, assessed and documented?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Requirements Definitions	AAT-14	Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	8
Artificial & Autonomous Technologies	AI & Autonomous Technologies Implementation Tasks Definition	AAT-14.1	Mechanisms exist to define the tasks that Artificial Intelligence (AI) and Autonomous Technologies (AAT) will support (e.g., classifiers, generative models, recommenders).			Does the organization define the tasks that Artificial Intelligence (AI) and Autonomous Technologies (AAT) will support (e?g?, classifiers, generative models, recommenders)?	8
Artificial & Autonomous Technologies	AI & Autonomous Technologies Knowledge Limits	AAT-14.2	Mechanisms exist to identify and document knowledge limits of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to provide sufficient information to assist relevant stakeholder decision making.			Does the organization identify and document knowledge limits of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to provide sufficient information to assist relevant stakeholder decision making?	10
Artificial & Autonomous Technologies	AI & Autonomous Technologies Viability Decisions	AAT-15	Mechanisms exist to define the criteria as to whether Artificial Intelligence (AI) and Autonomous Technologies (AAT) achieved intended purposes and stated objectives to determine whether its development or deployment should proceed.			Does the organization define the criteria as to whether Artificial Intelligence (AI) and Autonomous Technologies (AAT) achieved intended purposes and stated objectives to determine whether its development or deployment should proceed?	10
Artificial & Autonomous Technologies	AI & Autonomous Technologies Negative Residual Risks	AAT-15.1	Mechanisms exist to identify and document negative, residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers and end users of Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization identify and document negative, residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers and end users of Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	9
Artificial & Autonomous Technologies	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.			Does the organization define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Artificial & Autonomous Technologies	AI & Autonomous Technologies Production Monitoring	AAT-16	Mechanisms exist to monitor the functionality and behavior of the deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization monitor the functionality and behavior of the deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Measurement Approaches	AAT-16.1	Mechanisms exist to measure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks to deployment context(s) through review and consultation with industry experts, domain specialists and end users.			Does the organizationmeasure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks to deployment context(s) through review and consultation with industry experts, domain specialists and end users?	8
Artificial & Autonomous Technologies	Measuring AI & Autonomous Technologies Effectiveness	AAT-16.2	Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities.			Does the organization regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities?	5
Artificial & Autonomous Technologies	Unmeasurable AI & Autonomous Technologies Risks	AAT-16.3	Mechanisms exist to identify and document unmeasurable risks or trustworthiness characteristics.			Does the organization identify and document unmeasurable risks or trustworthiness characteristics?	7
Artificial & Autonomous Technologies	Efficacy of AI & Autonomous Technologies Measurement	AAT-16.4	Mechanisms exist to gather and assess feedback about the efficacy of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related measurements.			Does the organization gather and assess feedback about the efficacy of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related measurements?	5
Artificial & Autonomous Technologies	AI & Autonomous Technologies Domain Expert Reviews	AAT-16.5	Mechanisms exist to utilize input from domain experts and relevant stakeholders to validate whether the Artificial Intelligence (AI) and Autonomous Technologies (AAT) perform consistently, as intended.			Does the organization utilize input from domain experts and relevant stakeholders to validate whether the Artificial Intelligence (AI) and Autonomous Technologies (AAT) perform consistently, as intended?	8
Artificial & Autonomous Technologies	AI & Autonomous Technologies Performance Changes	AAT-16.6	Mechanisms exist to evaluate performance improvements or declines with domain experts and relevant stakeholders to define context-relevant risks and trustworthiness issues.			Does the organization evaluate performance improvements or declines with domain experts and relevant stakeholders to define context-relevant risks and trustworthiness issues?	10
Artificial & Autonomous Technologies	Pre-Trained AI & Autonomous Technologies Models	AAT-16.7	Mechanisms exist to validate the information sources and quality of pre-trained models used in Artificial Intelligence (AI) and Autonomous Technologies (AAT training, maintenance and improvement-related activities.			Does the organization validate the information sources and quality of pre-trained models used in Artificial Intelligence (AI) and Autonomous Technologies (AAT training, maintenance and improvement-related activities?	8
Artificial & Autonomous Technologies	AI & Autonomous Technologies Harm Prevention	AAT-17	Mechanisms exist to proactively prevent harm by regularly identifying and tracking existing, unanticipated and emergent Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.			Does the organization proactively prevent harm by regularly identifying and tracking existing, unanticipated and emergent Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks?	10
Artificial & Autonomous Technologies	AI & Autonomous Technologies Human Subject Protections	AAT-17.1	Mechanisms exist to protect human subjects from harm.			Does the organization protect human subjects from harm?	10
Artificial & Autonomous Technologies	AI & Autonomous Technologies Environmental Impact & Sustainability	AAT-17.2	Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT).			Does the organization assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	9
Artificial & Autonomous Technologies	Previously Unknown AI & Autonomous Technologies Threats & Risks	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.			Does the organization respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified?	9
Artificial & Autonomous Technologies	AI & Autonomous Technologies Risk Tracking Approaches	AAT-18	Mechanisms exist to track Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.			Does the organization track Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are difficult to assess using currently available measurement techniques or where metrics are not yet available?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Artificial & Autonomous Technologies	AI & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.			Does the organization prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output?	10
Asset Management	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	- Generally Accepted Accounting Principles (GAAP) - ITIL - Configuration Management Database (CMDB) - IT Asset Management (ITAM) program	E-AST-01	Does the organization facilitate the implementation of asset management controls?	10
Asset Management	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.		E-BCM-09	Does the organization identify and assess the security of technology assets that support more than one critical business function?	5
Asset Management	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical systems, applications and services to support the ongoing secure management of those assets.		E-CPL-03	Does the organization identify and involve pertinent stakeholders of critical systems, applications and services to support the ongoing secure management of those assets?	5
Asset Management	Standardized Naming Convention	AST-01.3	Mechanisms exist to implement a scalable, standardized naming convention for systems, applications and services that avoids asset naming conflicts.			Does the organization implement a scalable, standardized naming convention for systems, applications and services that avoids asset naming conflicts?	5
Asset Management	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: • Accurately reflects the current systems, applications and services in use; • Identifies authorized software products, including business justification details; • Is at the level of granularity deemed necessary for tracking and reporting; • Includes organization-defined information deemed necessary to achieve effective property accountability;	- ManageEngine AssetExplorer - LANDesk IT Asset Management Suite - ServiceNow (https://www.servicenow.com/) - Solarwinds (https://www.solarwinds.com/) - CrowdStrike	E-AST-04 E-AST-05 E-AST-07	Does the organization inventory technology assets that: • Accurately reflects the current system; • Is at the level of granularity deemed necessary for tracking and reporting; • Includes organization-defined information deemed necessary to achieve effective property accountability; and	10
Asset Management	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	- CrowdStrike - JAMF - ITIL - Configuration Management Database (CMDB)		Does the organization update asset inventories as part of component installations, removals and asset upgrades?	7
Asset Management	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - DHCP logging - Active discovery tools - NNT Change Tracker		Does the organization use automated mechanisms to detect and alert upon the detection of unauthorized hardware, software and firmware components?	3
Asset Management	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	- ITIL - Configuration Management Database (CMDB) - Manual or automated process		Does the organization prevent system components from being duplicated in other asset inventories?	2
Asset Management	Approved Baseline Deviations	AST-02.4	Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com) - Tripwire Enterprise	E-RSK-03 E-TDA-14	Does the organization document and govern instances of approved deviations from established baseline configurations?	8
Asset Management	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, that is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	- Cisco NAC - Aruba Networks - Juniper NAC - Packet Fence - Symantec NAC		Does the organization employ Network Access Control (NAC), or a similar technology, that is capable of detecting unauthorized devices and disable network access to those unauthorized devices?	4
Asset Management	Dynamic Host Configuration Protocol (DHCP) Server Logging	AST-02.6	Mechanisms exist to enable Dynamic Host Configuration Protocol (DHCP) server logging to improve asset inventories and assist in detecting unknown systems.	- Splunk - Manual Process - Build Automation Tools - NNT Log Tracker (https://www.newnettechnologies.com/event-log-	E-MON-04	Does the organization enable Dynamic Host Configuration Protocol (DHCP) server logging to improve asset inventories and assist in detecting unknown systems?	3
Asset Management	Software Licensing Restrictions	AST-02.7	Mechanisms exist to protect Intellectual Property (IP) rights with software licensing restrictions.	- Manual Process - Tripwire Enterprise (https://www.tripwire.com/products/tripwire-enterprise/)		Does the organization protect Intellectual Property (IP) rights with software licensing restrictions?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Asset Management	Data Action Mapping	AST-02.8	Mechanisms exist to create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed.	- Visio - LucidChart	E-DCH-05	Does the organization create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed?	9
Asset Management	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	- Configuration Management Database (CMDB)		Does the organization implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information?	5
Asset Management	Automated Location Tracking	AST-02.10	Mechanisms exist to track the geographic location of system components.			Does the organization track the geographic location of system components?	5
Asset Management	Component Assignment	AST-02.11	Mechanisms exist to bind components to a specific system.			Does the organization bind components to a specific system?	3
Asset Management	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.		E-AST-01 E-CPL-03	Does the organization assign asset ownership responsibilities to a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection?	8
Asset Management	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.		E-AST-01	Does the organization include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process?	5
Asset Management	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.		E-AST-22	Does the organization govern the chronology of the origin, development, ownership, location and changes to a system, system components and associated data?	8
Asset Management	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: • Contain sufficient detail to assess the security of the network's architecture; • Reflect the current architecture of the network environment; and • Document all sensitive/regulated data flows.	- High-Level Diagram (HLD) - Low-Level Diagram (LLD) - Data Flow Diagram (DFD) - Solarwinds (https://www.solarwinds.com/) - Paessler	E-DCH-03 E-DCH-04 E-DCH-05	Does the organization maintain network architecture diagrams that: • Contain sufficient detail to assess the security of the network's architecture; • Reflect the current architecture of the network environment; and • Document all sensitive/regulated data flows?	10
Asset Management	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity and privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).		E-AST-02 E-CPL-02 E-DCH-01 E-DCH-02	Does the organization determine cybersecurity and privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties)?	8
Asset Management	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.		E-AST-02 E-CPL-02	Does the organization ensure control applicability is appropriately-determined for systems, applications, services and third parties by graphically representing applicable boundaries?	6
Asset Management	Compliance-Specific Asset Identification	AST-04.3	Mechanisms exist to create and maintain a current inventory of systems, applications and services that are in scope for statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.		E-AST-02 E-CPL-02	Does the organization create and maintain a current inventory of systems, applications and services that are in scope for statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization?	6
Asset Management	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	- ITIL - Configuration Management Database (CMDB) - Definitive Software Library (DSL)		Does the organization maintain strict control over the internal or external distribution of any kind of sensitive/regulated media?	8
Asset Management	Management Approval For External Media Transfer	AST-05.1	Mechanisms exist to obtain management approval for any sensitive / regulated media that is transferred outside of the organization's facilities.			Does the organization obtain management approval for any sensitive / regulated media that is transferred outside of the organization's facilities?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Asset Management	Unattended End-User Equipment	AST-06	Mechanisms exist to implement enhanced protection measures for unattended systems to protect against tampering and unauthorized access.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - File Integrity Monitoring (FIM) - Lockable casings - Tamper detection tape		Does the organization implement enhanced protection measures for unattended systems to protect against tampering and unauthorized access?	9
Asset Management	Asset Storage In Automobiles	AST-06.1	Mechanisms exist to educate users on the need to physically secure laptops and other mobile devices out of site when traveling, preferably in the trunk of a vehicle.	- Security awareness training - Gamification		Does the organization educate users on the need to physically secure laptops and other mobile devices out of site when traveling, preferably in the trunk of a vehicle?	7
Asset Management	Kiosks & Point of Interaction (PoI) Devices	AST-07	Mechanisms exist to appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - File Integrity Monitoring (FIM) - Lockable casings - Tamper detection tape		Does the organization appropriately protect devices that capture sensitive/regulated data via direct physical interaction from tampering and substitution?	8
Asset Management	Tamper Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	- "Burner" phones & laptops - Tamper tape		Does the organization periodically inspect systems and system components for Indicators of Compromise (IoC)?	9
Asset Management	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	- Shred-it - IronMountain - sdelete (sysinternals) - Bootnukem	E-AST-03	Does the organization securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent such components from entering the gray market?	10
Asset Management	Return of Assets	AST-10	Mechanisms exist to ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement.	- Termination checklist - Manual Process - Native OS and Device Asset Tracking capabilities	E-AST-01	Does the organization ensure that employees and third-party users return all organizational assets in their possession upon termination of employment, contract or agreement?	8
Asset Management	Removal of Assets	AST-11	Mechanisms exist to authorize, control and track technology assets entering and exiting organizational facilities.	- RFID asset tagging - RFID proximity sensors at access points - Asset management software		Does the organization authorize, control and track technology assets entering and exiting organizational facilities?	8
Asset Management	Use of Personal Devices	AST-12	Mechanisms exist to restrict the possession and usage of personally-owned technology devices within organization-controlled facilities.	- BYOD policy		Does the organization restrict the possession and usage of personally-owned technology devices within organization-controlled facilities?	10
Asset Management	Use of Third-Party Devices	AST-13	Mechanisms exist to reduce the risk associated with third-party assets that are attached to the network from harming organizational assets or exfiltrating organizational data.	- NAC - Separate SSIDs for wireless networks - SIEM monitoring/alerting - Manual process to disable network all unused ports - Network Access Control (NAC)		Does the organization reduce the risk associated with third-party assets that are attached to the network from harming organizational assets or exfiltrating organizational data?	9
Asset Management	Usage Parameters	AST-14	Mechanisms exist to monitor and enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of system parameters.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization monitor and enforce usage parameters that limit the potential damage caused from the unauthorized or unintentional alteration of system parameters?	7
Asset Management	Bluetooth & Wireless Devices	AST-14.1	Mechanisms exist to prevent the usage of Bluetooth and wireless devices (e.g., Near Field Communications (NFC)) in sensitive areas or unless used in a Radio Frequency (RF)-screened building.			Does the organization prevent the usage of Bluetooth and wireless devices (e.g., Near Field Communications (NFC)) in sensitive areas or unless used in a Radio Frequency (RF)-screened building?	7
Asset Management	Infrared Communications	AST-14.2	Mechanisms exist to prevent line of sight and reflected infrared (IR) communications use in an unsecured space.			Does the organization prevent line of sight and reflected infrared (IR) communications travelling into an unsecured space?	5
Asset Management	Tamper Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Tamper detection tape - File Integrity Monitoring (FIM) - NNT Change Tracker		Does the organization verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle?	6

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Asset Management	Inspection of Systems, Components & Devices	AST-15.1	Mechanisms exist to physically and logically inspect critical technology assets to detect evidence of tampering.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Tamper detection tape - File Integrity Monitoring (FIM) - NNT Change Tracker		Does the organization physically and logically inspect critical systems to detect evidence of tampering?	6
Asset Management	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	- AirWatch - SCCM - Casper - BYOD policy		Does the organization implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace?	10
Asset Management	Prohibited Equipment & Services	AST-17	Mechanisms exist to govern Supply Chain Risk Management (SCRM) sanctions that require the removal and prohibition of certain technology services and/or equipment that are designated as supply chain threats by a statutory or regulatory body.		E-AST-10	Does the organization govern Supply Chain Risk Management (SCRM) sanctions that require the removal and prohibition of certain technology services and/or equipment that are designated as supply chain threats by a statutory or regulatory body?	9
Asset Management	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.			Does the organization provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification?	4
Asset Management	Telecommunications Equipment	AST-19	Mechanisms exist to establish usage restrictions and implementation guidance for telecommunication equipment to prevent potential damage or unauthorized modification and to prevent potential eavesdropping.			Does the organization establish usage restrictions and implementation guidance for telecommunication equipment based on the potential to cause damage, if used maliciously?	9
Asset Management	Video Teleconference (VTC) Security	AST-20	Mechanisms exist to implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms, to prevent potential eavesdropping.			Does the organization implement secure Video Teleconference (VTC) capabilities on endpoint devices and in designated conference rooms?	8
Asset Management	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.			Does the organization implement secure Internet Protocol (IP) telephony that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks?	8
Asset Management	Microphones & Web Cameras	AST-22	Mechanisms exist to configure assets to prohibit the use of endpoint-based microphones and web cameras in secure areas or where sensitive information is discussed.			Does the organization configure assets to prohibit the use of endpoint-based microphones and web cameras in secure areas or where sensitive information is discussed?	8
Asset Management	Multi-Function Devices (MFD)	AST-23	Mechanisms exist to securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device.		E-TPM-01	Does the organization securely configure Multi-Function Devices (MFD) according to industry-recognized secure practices for the type of device?	8
Asset Management	Travel-Only Devices	AST-24	Mechanisms exist to issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.			Does the organization issue personnel travelling overseas with temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies?	8
Asset Management	Re-Imaging Devices After Travel	AST-25	Mechanisms exist to re-image end user technology (e.g., laptops and mobile devices) when returning from overseas travel to an authoritarian country with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.			Does the organization re-image end user technology (e.g., laptops and mobile devices) when returning from overseas travel to an authoritarian country with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies?	8
Asset Management	System Administrative Processes	AST-26	Mechanisms exist to develop, implement and govern system administration processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining systems, applications and services.			Does the organization develop, implement and govern system administration processes with corresponding Standardized Operating Procedures (SOP) for operating and maintaining systems, applications and services?	9
Asset Management	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.			Does the organization conduct remote system administrative functions via a "jump box" or "jump server" that is located in a separate network zone to user workstations?	7

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Asset Management	Database Administrative Processes	AST-28	Mechanisms exist to develop, implement and govern database management processes, with corresponding Standardized Operating Procedures (SOP), for operating and maintaining databases.			Does the organization develop, implement and govern database management processes with corresponding Standardized Operating Procedures (SOP) for operating and maintaining databases?	9
Asset Management	Database Management System (DBMS)	AST-28.1	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.			Does the organization implement and maintain a Database Management System (DBMS)?	6
Asset Management	Radio Frequency Identification (RFID) Security	AST-29	Mechanisms exist to securely govern Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.			Does the organization securely governs Radio Frequency Identification (RFID) deployments to ensure RFID is used safely and securely to protect the confidentiality and integrity of data and prevent the compromise of secure spaces?	3
Asset Management	Contactless Access Control Systems	AST-29.1	Mechanisms exist to securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces.			Does the organization securely configure contactless access control systems incorporating contactless RFID or smart cards to protect the confidentiality and integrity of data and prevent the compromise of secure spaces?	3
Asset Management	Decommissioning	AST-30	Mechanisms exist to ensure systems, applications and services are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.			Does the organization ensure systems, applications and services are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations?	4
Asset Management	Asset Categorization	AST-31	Mechanisms exist to categorize technology assets.		E-AST-24	Does the organization categorize technology assets?	9
Asset Management	Categorize Artificial Intelligence (AI)-Related Technologies	AST-31.1	Mechanisms exist to categorize Artificial Intelligence (AI) and Autonomous Technologies (AAT).		E-AST-24	Does the organization categorize Artificial Intelligence (AI) and Autonomous Technologies (AAT)?	9
Business Continuity & Disaster Recovery	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services.	- Business Continuity Plan (BCP) - Disaster Recovery Plan (DRP) - Continuity of Operations Plan (COOP) - Business Impact Analysis (BIA) - Criticality assessments	E-BCM-01	Does the organization facilitate the implementation of contingency planning controls?	10
Business Continuity & Disaster Recovery	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	- Cybersecurity Incident Response Plan (IIRP)		Does the organization coordinate contingency plan development with internal and external elements responsible for related plans?	5
Business Continuity & Disaster Recovery	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	- Business Continuity Plan (BCP) - Disaster Recovery Plan (DRP) - Continuity of Operations Plan (COOP)		Does the organization coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied?	5
Business Continuity & Disaster Recovery	Transfer to Alternate Processing / Storage Site	BCD-01.3	Mechanisms exist to redeploy personnel to other roles during a disruptive event or in the execution of a continuity plan.			Does the organization redeploy personnel to other roles during a disruptive event or in the execution of a continuity plan?	5
Business Continuity & Disaster Recovery	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).		E-BCM-02 E-BCM-03	Does the organization configure the alternate storage site to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)?	5
Business Continuity & Disaster Recovery	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical systems, applications and services that support essential missions and business functions.	- Business Impact Analysis (BIA) - Criticality assessments	E-BCM-08	Does the organization identify and document the critical systems, applications and services that support essential missions and business functions?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Business Continuity & Disaster Recovery	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.	- Disaster Recovery Plan (DRP) - Continuity of Operations Plan (COOP) - Disaster recovery software		Does the organization plan for the resumption of all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation?	8
Business Continuity & Disaster Recovery	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.	- Disaster Recovery Plan (DRP) - Continuity of Operations Plan (COOP)		Does the organization plan for the continuance of 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?	8
Business Continuity & Disaster Recovery	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	- Business Continuity Plan (BCP) - Disaster Recovery Plan (DRP) - Continuity of Operations Plan (COOP)		Does the organization resume essential missions and business functions within an organization-defined time period of contingency plan activation?	8
Business Continuity & Disaster Recovery	Data Storage Location Reviews	BCD-02.4	Mechanisms exist to perform periodic security reviews of storage locations that contain sensitive / regulated data.		E-AST-23	Does the organization perform periodic security reviews of storage locations that contain sensitive / regulated data?	8
Business Continuity & Disaster Recovery	Contingency Training	BCD-03	Mechanisms exist to adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities.	- NIST NICE Framework - Tabletop exercises	E-BCM-07	Does the organization adequately train contingency personnel and applicable stakeholders in their contingency roles and responsibilities?	5
Business Continuity & Disaster Recovery	Simulated Events	BCD-03.1	Mechanisms exist to incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.	- Tabletop exercises	E-BCM-06	Does the organization incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations?	3
Business Continuity & Disaster Recovery	Automated Training Environments	BCD-03.2	Automated mechanisms exist to provide a more thorough and realistic contingency training environment.			Does the organization use automated mechanisms to provide a more thorough and realistic contingency training environment?	1
Business Continuity & Disaster Recovery	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	- Simulated disasters / emergencies	E-BCM-06 E-BCM-07	Does the organization conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan?	6
Business Continuity & Disaster Recovery	Coordinated Testing with Related Plans	BCD-04.1	Mechanisms exist to coordinate contingency plan testing with internal and external elements responsible for related plans.	- Playbooks - Enterprise-wide Continuity of Operations Plan (COOP)		Does the organization coordinate contingency plan testing with internal and external elements responsible for related plans?	3
Business Continuity & Disaster Recovery	Alternate Storage & Processing Sites	BCD-04.2	Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations.			Does the organization test the contingency plan at the alternate processing site to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations?	5
Business Continuity & Disaster Recovery	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	- Standardized Operating Procedures (SOP) - Disaster Recovery Plan (DRP) - Business Continuity Plan (BCP) - Continuity of Operations Plan (COOP)	E-BCM-04	Does the organization conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated?	9
Business Continuity & Disaster Recovery	Contingency Planning & Updates	BCD-06	Mechanisms exist to keep contingency plans current with business needs, technology changes and feedback from contingency plan testing activities.	- Offline / offsite documentation	E-BCM-05	Does the organization keep contingency plans current with business needs, technology changes and feedback from contingency plan testing activities?	8
Business Continuity & Disaster Recovery	Alternative Security Measures	BCD-07	Mechanisms exist to implement alternative or compensating controls to satisfy security functions when the primary means of implementing the security function is unavailable or compromised.	- Business Impact Analysis (BIA) - Criticality assessments		Does the organization implement alternative or compensating controls to satisfy security functions when the primary means of implementing the security function is unavailable or compromised?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Business Continuity & Disaster Recovery	Alternate Storage Site	BCD-08	Mechanisms exist to establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information.	- SunGard - AWS - Azure		Does the organization establish an alternate storage site that includes both the assets and necessary agreements to permit the storage and recovery of system backup information?	9
Business Continuity & Disaster Recovery	Separation from Primary Site	BCD-08.1	Mechanisms exist to separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats.	- SunGard - AWS - Azure		Does the organization separate the alternate storage site from the primary storage site to reduce susceptibility to similar threats?	7
Business Continuity & Disaster Recovery	Accessibility	BCD-08.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster.	- SunGard - AWS - Azure		Does the organization identify and mitigate potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster?	5
Business Continuity & Disaster Recovery	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	- SunGard - AWS - Azure		Does the organization establish an alternate processing site that provides security measures equivalent to that of the primary site?	9
Business Continuity & Disaster Recovery	Separation from Primary Site	BCD-09.1	Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats.	- SunGard - AWS - Azure		Does the organization separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats?	7
Business Continuity & Disaster Recovery	Accessibility	BCD-09.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing site and possible mitigation actions, in the event of an area-wide disruption or disaster.	- Business Continuity Plan (BCP) - Continuity of Operations Plan (COOP)		Does the organization identify potential accessibility problems to the alternate processing site and possible mitigation actions, in the event of an area-wide disruption or disaster?	5
Business Continuity & Disaster Recovery	Alternate Site Priority of Service	BCD-09.3	Mechanisms exist to address priority-of-service provisions in alternate processing and storage sites that support availability requirements, including Recovery Time Objectives (RTOs).	- Hot / warm / cold site contracts	E-TPM-04	Does the organization address priority-of-service provisions in alternate processing and storage sites that support availability requirements, including Recovery Time Objectives (RTOs)?	6
Business Continuity & Disaster Recovery	Preparation for Use	BCD-09.4	Mechanisms exist to prepare the alternate processing alternate to support essential missions and business functions so that the alternate site is capable of being used as the primary site.			Does the organization prepare the alternate processing alternate to support essential missions and business functions so that the alternate site is capable of being used as the primary site?	5
Business Continuity & Disaster Recovery	Inability to Return to Primary Site	BCD-09.5	Mechanisms exist to plan and prepare for both natural and manmade circumstances that preclude returning to the primary processing site.			Does the organization plan and prepare for both natural and manmade circumstances that preclude returning to the primary processing site?	5
Business Continuity & Disaster Recovery	Telecommunications Services Availability	BCD-10	Mechanisms exist to reduce the likelihood of a single point of failure with primary telecommunications services.	- Alternate telecommunications services are maintained with multiple ISP / network providers		Does the organization reduce the likelihood of a single point of failure with primary telecommunications services?	6
Business Continuity & Disaster Recovery	Telecommunications Priority of Service Provisions	BCD-10.1	Mechanisms exist to formalize primary and alternate telecommunications service agreements contain priority-of-service provisions that support availability requirements, including Recovery Time Objectives (RTOs).	- Hot / warm / cold site contracts	E-TPM-04	Does the organization formalize primary and alternate telecommunications service agreements contain priority-of-service provisions that support availability requirements, including Recovery Time Objectives (RTOs)?	6
Business Continuity & Disaster Recovery	Separation of Primary / Alternate Providers	BCD-10.2	Mechanisms exist to obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.			Does the organization obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats?	5
Business Continuity & Disaster Recovery	Provider Continency Plan	BCD-10.3	Mechanisms exist to contractually-require telecommunications service providers to have contingency plans that meet organizational contingency requirements.			Does the organization contractually-require telecommunications service providers to have contingency plans that meet organizational contingency requirements?	5

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Business Continuity & Disaster Recovery	Alternate Communications Paths	BCD-10.4	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable.			Does the organization maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable?	5
Business Continuity & Disaster Recovery	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).	- Backup technologies & procedures - Offline storage	E-BCM-10 E-BCM-11 E-BCM-12 E-BCM-13	Does the organization 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)?	10
Business Continuity & Disaster Recovery	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.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data?	9
Business Continuity & Disaster Recovery	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.	- IronMountain	E-AST-08 E-BCM-11 E-BCM-12 E-BCM-13	Does the organization store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up?	8
Business Continuity & Disaster Recovery	Information System Imaging	BCD-11.3	Mechanisms exist to reimage assets from configuration-controlled and integrity-protected images that represent a secure, operational state.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Acronis - Docker (https://www.docker.com/) - VMWare		Does the organization reimage assets from configuration-controlled and integrity-protected images that represent a secure, operational state?	8
Business Continuity & Disaster Recovery	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	- Backup technologies & procedures		Are cryptographic mechanisms utilized to prevent the unauthorized disclosure and/or modification of backup information/	9
Business Continuity & Disaster Recovery	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.			Does the organization utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing?	5
Business Continuity & Disaster Recovery	Transfer to Alternate Storage Site	BCD-11.6	Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).			Does the organization transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)?	5
Business Continuity & Disaster Recovery	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover system, that is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.			Does the organization maintain a failover system, that is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations?	5
Business Continuity & Disaster Recovery	Dual Authorization For Backup Media Destruction	BCD-11.8	Mechanisms exist to implement and enforce dual authorization for the deletion or destruction of sensitive backup media and data.			Does the organization implement and enforce dual authorization for the deletion or destruction of sensitive backup media and data?	5
Business Continuity & Disaster Recovery	Backup Access	BCD-11.9	Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations.			Does the organization restrict access to backups to privileged users with assigned roles for data backup and recovery operations?	9
Business Continuity & Disaster Recovery	Backup Modification and/or Destruction	BCD-11.10	Mechanisms exist to restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles.			Does the organization restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles?	9
Business Continuity & Disaster Recovery	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Business Continuity & Disaster Recovery	Transaction Recovery	BCD-12.1	Mechanisms exist to utilize specialized backup mechanisms that will allow transaction recovery for transaction-based applications and services in accordance with Recovery Point Objectives (RPOs).			Does the organization utilize specialized backup mechanisms that will allow transaction recovery for transaction-based applications and services in accordance with Recovery Point Objectives (RPOs)?	9
Business Continuity & Disaster Recovery	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical systems, applications and/or services.	- Load balancers - High Availability (HA) firewalls		Does the organization implement real-time or near-real-time failover capability to maintain availability of critical systems, applications and/or services?	8
Business Continuity & Disaster Recovery	Electronic Discovery (eDiscovery)	BCD-12.3	Mechanisms exist to utilize electronic discovery (eDiscovery) that covers current and archived communication transactions.			Does the organization utilize electronic discovery (eDiscovery) that covers current and archived communication transactions?	8
Business Continuity & Disaster Recovery	Restore Within Time Period	BCD-12.4	Mechanisms exist to restore systems, applications and/or services within organization-defined restoration time-periods from configuration-controlled and integrity-protected information; representing a known, operational state for the asset.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization restore systems, applications and/or services within organization-defined restoration time-periods from configuration-controlled and integrity-protected information; representing a known, operational state for the asset?	5
Business Continuity & Disaster Recovery	Backup & Restoration Hardware Protection	BCD-13	Mechanisms exist to protect backup and restoration hardware and software.			Does the organization protect backup and restoration hardware and software?	8
Business Continuity & Disaster Recovery	Isolated Recovery Environment	BCD-14	Mechanisms exist to utilize an isolated, non-production environment to perform data backup and recovery operations through offline, cloud or off-site capabilities.			Does the organization utilize an isolated, non-production environment to perform data backup and recovery operations through offline, cloud or off-site capabilities?	5
Business Continuity & Disaster Recovery	Reserve Hardware	BCD-15	Mechanisms exist to purchase and maintain a sufficient reserve of spare hardware to ensure essential missions and business functions can be maintained in the event of a supply chain disruption.			Does the organization purchase and maintain a sufficient reserve of spare hardware to ensure essential missions and business functions can be maintained in the event of a supply chain disruption?	7
Business Continuity & Disaster Recovery	AI & Autonomous Technologies Incidents	BCD-16	Mechanisms exist to handle failures or incidents with Artificial Intelligence (AI) and Autonomous Technologies (AAT) deemed to be high-risk.			Does the organization handle failures or incidents with Artificial Intelligence (AI) and Autonomous Technologies (AAT) deemed to be high-risk?	10
Capacity & Performance Planning	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	- Splunk - Resource monitoring		Does the organization facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements?	8
Capacity & Performance Planning	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	- Splunk - Resource monitoring		Does the organization control resource utilization of systems that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources?	8
Capacity & Performance Planning	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.			Does the organization conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations?	8
Capacity & Performance Planning	Performance Monitoring	CAP-04	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical systems, applications and services.			Does the organization centrally-monitor and alert on the operating state and health status of critical systems, applications and services?	7
Change Management	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - VisibleOps methodology - ITIL infrastructure library - NNT Change Tracker	E-CHG-02	Does the organization facilitate the implementation of a change management program?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Change Management	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Change Control Board (CCB) - Configuration Management Database (CMDB) - Tripwire Enterprise	E-CHG-02	Does the organization govern the technical configuration change control processes?	8
Change Management	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - VisibleOps methodology - ITIL infrastructure library - Manual processes/workflows		Does the organization prohibit unauthorized changes, unless organization-approved change requests are received?	10
Change Management	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - VisibleOps methodology - ITIL infrastructure library - NNT Change Tracker	E-CHG-03	Does the organization appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment?	9
Change Management	Security & Privacy Representative for Asset Lifecycle Changes	CHG-02.3	Mechanisms exist to include a cybersecurity and/or privacy representative in the configuration change control review process.	- Change Control Board (CCB) - Change Advisory Board (CAB) - VisibleOps methodology - ITIL infrastructure library	E-CHG-04	Does the organization include a cybersecurity representative in the configuration change control review process?	7
Change Management	Automated Security Response	CHG-02.4	Automated mechanisms exist to implement remediation actions upon the detection of unauthorized baseline configurations change(s).	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization implement remediation actions upon the detection of unauthorized baseline configurations change(s)?	5
Change Management	Cryptographic Management	CHG-02.5	Mechanisms exist to govern assets involved in providing cryptographic protections according to the organization's configuration management processes.			Does the organization govern assets involved in providing cryptographic protections according to the organization's configuration management processes?	5
Change Management	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	- VisibleOps methodology - ITIL infrastructure library - Change management software		Does the organization analyze proposed changes for potential security impacts, prior to the implementation of the change?	9
Change Management	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - VisibleOps methodology - ITIL infrastructure library - Role-based permissions		Does the organization enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes?	8
Change Management	Automated Access Enforcement / Auditing	CHG-04.1	Mechanisms exist to perform after-the-fact reviews of configuration change logs to discover any unauthorized changes.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - VisibleOps methodology - ITIL infrastructure library - NNT Change Tracker		Does the organization perform after-the-fact reviews of configuration change logs to discover any unauthorized changes?	3
Change Management	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	- Privileged Account Management (PAM) - Patch management tools - OS configuration standards		Does the organization prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority?	3
Change Management	Dual Authorization for Change	CHG-04.3	Mechanisms exist to enforce a two-person rule for implementing changes to critical assets.	- Separation of Duties (SoD)		Does the organization enforce a two-person rule for implementing changes to critical assets?	6
Change Management	Limit Production / Operational Privileges (Incompatible Roles)	CHG-04.4	Mechanisms exist to limit operational privileges for implementing changes.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Separation of Duties (SoD) - Privileged Account Management (PAM)		Does the organization limit operational privileges for implementing changes?	6
Change Management	Library Privileges	CHG-04.5	Mechanisms exist to restrict software library privileges to those individuals with a pertinent business need for access.	- Privileged Account Management (PAM)		Does the organization restrict software library privileges to those individuals with a pertinent business need for access?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Change Management	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	- Change management procedures - VisibleOps methodology - ITIL infrastructure library		Does the organization ensure stakeholders are made aware of and understand the impact of proposed changes?	9
Change Management	Security Functionality Verification	CHG-06	Mechanisms exist to verify the functionality of security controls when anomalies are discovered.	- Information Assurance Program (IAP) - Security Test & Evaluation (STE)		Does the organization verify the functionality of security controls when anomalies are discovered?	9
Change Management	Report Verification Results	CHG-06.1	Mechanisms exist to report the results of cybersecurity and privacy function verification to appropriate organizational management.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization report the results of cybersecurity and privacy function verification to appropriate organizational management?	5
Cloud Security	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	- Data Protection Impact Assessment (DPIA)	E-AST-06	Does the organization facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices?	10
Cloud Security	Cloud Infrastructure Onboarding	CLD-01.1	Mechanisms exist to ensure cloud services are designed and configured so systems, applications and processes are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.			Does the organization ensure cloud services are designed and configured so systems, applications and processes are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations?	9
Cloud Security	Cloud Infrastructure Offboarding	CLD-01.2	Mechanisms exist to ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.			Does the organization ensure cloud services are decommissioned so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations?	9
Cloud Security	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	- Architectural review board - System Security Plan (SSP) - Security architecture roadmaps	E-TDA-09	Does the organization ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments?	8
Cloud Security	Cloud Infrastructure Security Subnet	CLD-03	Mechanisms exist to host security-specific technologies in a dedicated subnet.	- Security management subnet		Does the organization host security-specific technologies in a dedicated subnet?	6
Cloud Security	Application & Program Interface (API) Security	CLD-04	Mechanisms exist to ensure support for secure interoperability between components with Application & Program Interfaces (APIs).	- Use only open and published APIs		Does the organization ensure support for secure interoperability between components?	9
Cloud Security	Virtual Machine Images	CLD-05	Mechanisms exist to ensure the integrity of virtual machine images at all times.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - File Integrity Monitoring (FIM) - Docker (https://www.docker.com/) - NNT Change Tracker		Does the organization ensure the integrity of virtual machine images at all times?	8
Cloud Security	Multi-Tenant Environments	CLD-06	Mechanisms exist to ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.	- Security architecture review - Defined processes to segment at the network, application, databases layers		Does the organization ensure multi-tenant owned or managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users?	9
Cloud Security	Customer Responsibility Matrix (CRM)	CLD-06.1	Mechanisms exist to formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers.	- Customer Responsibility Matrix (CRM) - Shared Responsibility Matrix (SRM) - Responsible, Accountable, Supporting, Consulted and Informed (RASCI) matrix	E-CPL-03	Does the organization formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers?	8
Cloud Security	Multi-Tenant Event Logging Capabilities	CLD-06.2	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations.			Does the organization ensure Multi-Tenant Service Providers (MTSP) facilitate security event logging capabilities for its customers that are consistent with applicable statutory, regulatory and/or contractual obligations?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Cloud Security	Multi-Tenant Forensics Capabilities	CLD-06.3	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate prompt forensic investigations in the event of a suspected or confirmed security incident.			Does the organization ensure Multi-Tenant Service Providers (MTSP) facilitate prompt forensic investigations in the event of a suspected or confirmed security incident?	8
Cloud Security	Multi-Tenant Incident Response Capabilities	CLD-06.4	Mechanisms exist to ensure Multi-Tenant Service Providers (MTSP) facilitate prompt response to suspected or confirmed security incidents and vulnerabilities, including timely notification to affected customers.			Does the organization ensure Multi-Tenant Service Providers (MTSP) facilitate prompt response to suspected or confirmed security incidents and vulnerabilities, including timely notification to affected customers?	8
Cloud Security	Data Handling & Portability	CLD-07	Mechanisms exist to ensure cloud providers use secure protocols for the import, export and management of data in cloud-based services.	- Data Protection Impact Assessment (DPIA) - Security architecture review - Encrypted data transfers (e.g. TLS or VPNs)		Does the organization ensure cloud providers use secure protocols for the import, export and management of data in cloud-based services?	4
Cloud Security	Standardized Virtualization Formats	CLD-08	Mechanisms exist to ensure interoperability by requiring cloud providers to use industry-recognized formats and provide documentation of custom changes for review.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Data Protection Impact Assessment (DPIA) - Manual review process - Vendor risk assessments		Does the organization ensure interoperability by requiring cloud providers to use industry-recognized formats and provide documentation of custom changes for review?	4
Cloud Security	Geolocation Requirements for Processing, Storage and Service Locations	CLD-09	Mechanisms exist to control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.	- Data Protection Impact Assessment (DPIA)	E-AST-06 E-AST-23	Does the organization control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations?	10
Cloud Security	Sensitive Data In Public Cloud Providers	CLD-10	Mechanisms exist to limit and manage the storage of sensitive/regulated data in public cloud providers.	- Data Protection Impact Assessment (DPIA) - Security and network architecture diagrams - Data Flow Diagram (DFD)	E-AST-08	Does the organization limit and manage the storage of sensitive/regulated data in public cloud providers?	6
Cloud Security	Cloud Access Point (CAP)	CLD-11	Mechanisms exist to utilize Cloud Access Points (CAPs) to provide boundary protection and monitoring functions that both provide access to the cloud and protect the organization from the cloud.	- Next Generation Firewall (NGF) - Web Application Firewall (WAF) - Network Routing / Switching - Intrusion Detection / Protection (IDS / IPS) - Data Loss Prevention (DLP)		Does the organization utilize Cloud Access Points (CAPs) to provide boundary protection and monitoring functions that both provide access to the cloud and protect the organization from the cloud?	7
Cloud Security	Side Channel Attack Prevention	CLD-12	Mechanisms exist to prevent "side channel attacks" when using a Content Delivery Network (CDN) by restricting access to the origin server's IP address to the CDN and an authorized management network.			Does the organization prevent "side channel attacks" when using a Content Delivery Network (CDN) by restricting access to the origin server's IP address to the CDN and an authorized management network?	3
Compliance	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	- Governance, Risk and Compliance Solution (GRC) tool (SCFConnect, SureCloud,Ostendio, ZenGRC, Archer, RSAM, MetricStream, etc.) - Steering committee	E-CPL-01 E-GOV-10	Does the organization facilitate the implementation of relevant statutory, regulatory and contractual controls?	10
Compliance	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.		E-CPL-05	Does the organization document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions?	9
Compliance	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.		E-AST-02 E-CPL-02 E-GOV-10	Does the organization document and validate the scope of cybersecurity and privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations?	10
Compliance	Security & Privacy Controls Oversight	CPL-02	Mechanisms exist to provide a security & privacy controls oversight function that reports to the organization's executive leadership.	- Governance, Risk and Compliance Solution (GRC) tool (SCFConnect, SureCloud,Ostendio, ZenGRC, Archer, RSAM, MetricStream, etc.) - Steering committee - Formalized SDLC program	E-CPL-07 E-CPL-09 E-GOV-04 E-GOV-05 E-GOV-06 E-GOV-13	Does the organization provide a security & privacy controls oversight function that reports to the organization's executive leadership?	10
Compliance	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.		E-CPL-04 E-CPL-07	Does the organization implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes?	5

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Compliance	Security Assessments	CPL-03	Mechanisms exist to ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate security policies, standards and other applicable requirements.	- Information Assurance Program (IAP) - Security Test & Evaluation (STE) - Governance, Risk and Compliance Solution (GRC) tool (SCFConnect, SureCloud,Ostendio, ZenGRC, Archer, RSAM, MetricStream, etc.)	E-CPL-05 E-CPL-07	Does the organization ensure managers regularly review the processes and documented procedures within their area of responsibility to adhere to appropriate security policies, standards and other applicable requirements?	10
Compliance	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate security & privacy controls at planned intervals or when the system, service or project undergoes significant changes.	- Information Assurance Program (IAP) - Security Test & Evaluation (STE)	E-CPL-07	Does the organization utilize independent assessors to evaluate security & privacy controls at planned intervals or when the system, service or project undergoes significant changes?	6
Compliance	Functional Review Of Security Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and privacy policies and standards.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Internal audit program - NNT Change Tracker (https://www.newnettechnologies.com)	E-CPL-08	Does the organization regularly review technology assets for adherence to the organization's cybersecurity and privacy policies and standards?	8
Compliance	Audit Activities	CPL-04	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	- Internal audit program		Does the organization thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations?	5
Compliance	Legal Assessment of Investigative Inquires	CPL-05	Mechanisms exist to determine whether a government agency has an applicable and valid legal basis to request data from the organization and what further steps need to be taken, if necessary.			Does the organization determine whether a government agency has an applicable and valid legal basis to request data from the organization and what further steps need to be taken, if necessary?	2
Compliance	Investigation Request Notifications	CPL-05.1	Mechanisms exist to notify customers about investigation request notifications, unless the applicable legal basis for a government agency's action prohibits notification (e.g., potential criminal prosecution).			Does the organization notify customers about investigation request notifications, unless the applicable legal basis for a government agency's action prohibits notification (e.g., potential criminal prosecution)?	2
Compliance	Investigation Access Restrictions	CPL-05.2	Mechanisms exist to support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the data and systems needed to perform the investigation.			Does the organization support official investigations by provisioning government investigators with "least privileges" and "least functionality" to ensure that government investigators only have access to the data and systems needed to perform the investigation?	2
Compliance	Government Surveillance	CPL-06	Mechanisms exist to constrain the host government from having unrestricted and non-monitored access to the organization's systems, applications and services that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	- Board of Directors (Bod) Ethics Committee		Does the organization constrain the host government from having unrestricted and non-monitored access to the organization's systems, applications and services that could potentially violate other applicable statutory, regulatory and/or contractual obligations.	10
Configuration Management	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	- NNT Change Tracker (https://www.newnettechnologies.com) - Configuration Management Database (CMDB) - Baseline hardening standards - Formalized DevOps program		Does the organization facilitate the implementation of configuration management controls?	9
Configuration Management	Assignment of Responsibility	CFG-01.1	Mechanisms exist to implement a segregation of duties for configuration management that prevents developers from performing production configuration management duties.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization implement a segregation of duties for configuration management that prevents developers from performing production configuration management duties?	5
Configuration Management	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.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) - Center for Internet Security (CIS) Benchmarks	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17	Does the organization develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards?	10
Configuration Management	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: • At least annually; • When required due to so; or • As part of system component installations and upgrades.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Defense Information Security Agency (DISA) Secure Technology Implementation Guides (STIGs) - Center for Internet Security (CIS) Benchmarks		Does the organization review and update baseline configurations: • At least annually; • When required due to so; or • As part of system component installations and upgrades?	8
Configuration Management	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of the systems.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization use automated mechanisms to govern and report on baseline configurations of the systems?	7

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Configuration Management	Retention Of Previous Configurations	CFG-02.3	Mechanisms exist to retain previous versions of baseline configuration to support roll back.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization retain previous versions of baseline configuration to support roll back?	3
Configuration Management	Development & Test Environment Configurations	CFG-02.4	Mechanisms exist to manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization manage baseline configurations for development and test environments separately from operational baseline configurations to minimize the risk of unintentional changes?	5
Configuration Management	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.	- NNT Change Tracker (https://www.newnettechnologies.com)	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17	Does the organization configure systems utilized in high-risk areas with more restrictive baseline configurations?	8
Configuration Management	Network Device Configuration File Synchronization	CFG-02.6	Mechanisms exist to configure network devices to synchronize startup and running configuration files.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization configure network devices to synchronize startup and running configuration files?	7
Configuration Management	Approved Configuration Deviations	CFG-02.7	Mechanisms exist to document, assess risk and approve or deny deviations to standardized configurations.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization document, assess risk and approve or deny deviations to standardized configurations.	9
Configuration Management	Respond To Unauthorized Changes	CFG-02.8	Mechanisms exist to respond to unauthorized changes to configuration settings as security incidents.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Service Level Agreements (SLAs) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization respond to unauthorized changes to configuration settings as security incidents?	9
Configuration Management	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: • Mission / business functions; • Operational environment; • Specific threats or vulnerabilities; or	- DISA STIGs - CIS Benchmarks		Does the organization allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: • Mission / business functions; • Operational environment; • Specific threats or vulnerabilities; or	9
Configuration Management	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.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services?	10
Configuration Management	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	- NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services?	8
Configuration Management	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization use automated mechanisms to prevent the execution of unauthorized software programs?	7
Configuration Management	Unauthorized or Authorized Software (Blacklisting or Whitelisting)	CFG-03.3	Mechanisms exist to whitelist or blacklist applications in an order to limit what is authorized to execute on systems.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization whitelist or blacklist applications in an order to limit what is authorized to execute on systems?	5
Configuration Management	Split Tunneling	CFG-03.4	Mechanisms exist to prevent systems from creating split tunneling connections or similar techniques that could be used to exfiltrate data.			Does the organization prevent systems from creating split tunneling connections or similar techniques that could be used to exfiltrate data?	8
Configuration Management	Software Usage Restrictions	CFG-04	Mechanisms exist to enforce software usage restrictions to comply with applicable contract agreements and copyright laws.			Does the organization enforce software usage restrictions to comply with applicable contract agreements and copyright laws?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Configuration Management	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.	- Acceptable Use Policy (AUP)		Does the organization establish parameters for the secure use of open source software?	9
Configuration Management	Unsupported Internet Browsers & Email Clients	CFG-04.2	Mechanisms exist to allow only approved Internet browsers and email clients to run on systems.			Does the organization allow only approved Internet browsers and email clients to run on systems?	7
Configuration Management	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	- Privileged Account Management (PAM)		Does the organization restrict the ability of non-privileged users to install unauthorized software?	10
Configuration Management	Unauthorized Installation Alerts	CFG-05.1	Mechanisms exist to configure systems to generate an alert when the unauthorized installation of software is detected.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization configure systems to generate an alert when the unauthorized installation of software is detected?	8
Configuration Management	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.			Does the organization prohibit the installation of software, unless the action is performed by a privileged user or service?	9
Configuration Management	Configuration Enforcement	CFG-06	Automated mechanisms exist to monitor, enforce and report on configurations for endpoint devices.			Does the organization use automated mechanisms to monitor, enforce and report on configurations for endpoint devices?	7
Configuration Management	Zero-Touch Provisioning (ZTP)	CFG-07	Mechanisms exist to implement Zero-Touch Provisioning (ZTP), or similar technology, to automatically and securely configure devices upon being added to a network.			Does the organization implement Zero-Touch Provisioning (ZTP), or similar technology, to automatically and securely configure devices upon being added to a network?	8
Configuration Management	Sensitive / Regulated Data Access Enforcement	CFG-08	Mechanisms exist to configure systems, applications and processes to restrict access to sensitive/regulated data.		E-DCH-08	Does the organization configure systems, applications and processes to restrict access to sensitive/regulated data?	7
Configuration Management	Sensitive / Regulated Data Actions	CFG-08.1	Automated mechanisms exist to generate event logs whenever sensitive/regulated data is collected, created, updated, deleted and/or archived.			Does the organization ensure event logs are generated whenever sensitive/regulated data is collected, created, updated, deleted and/or archived?	7
Continuous Monitoring	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	- Splunk - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization facilitate the implementation of enterprise-wide monitoring controls?	10
Continuous Monitoring	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points?	9
Continuous Monitoring	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)	E-MON-01 E-MON-05	Does the organization utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation?	9
Continuous Monitoring	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Continuous Monitoring	System Generated Alerts	MON-01.4	Mechanisms exist to monitor, correlate and respond to alerts from physical, cybersecurity, privacy and supply chain activities to achieve integrated situational awareness.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization monitor, correlate and respond to alerts from physical, cybersecurity, privacy and supply chain activities to achieve integrated situational awareness?	7
Continuous Monitoring	Wireless Intrusion Detection System (WIDS)	MON-01.5	Mechanisms exist to utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) to identify rogue wireless devices and to detect attack attempts via wireless networks.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization utilize Wireless Intrusion Detection / Protection Systems (WIDS / WIPS) to identify rogue wireless devices and to detect attack attempts via wireless networks?	5
Continuous Monitoring	Host-Based Devices	MON-01.6	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS) to actively alert on or block unwanted activities and send logs to a Security Incident Event Manager (SIEM), or similar automated tool, to maintain situational awareness.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS) to actively alert on or block unwanted activities and send logs to a Security Incident Event Manager (SIEM), or similar automated tool, to maintain situational awareness?	8
Continuous Monitoring	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical assets to generate alerts for unauthorized modifications.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical assets to generate alerts for unauthorized modifications?	9
Continuous Monitoring	Reviews & Updates	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	- Security Incident Event Manager (SIEM) - Splunk	E-MON-01 E-MON-02 E-MON-05	Does the organization review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures?	10
Continuous Monitoring	Proxy Logging	MON-01.9	Mechanisms exist to log all Internet-bound requests, in order to identify prohibited activities and assist incident handlers with identifying potentially compromised systems.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization log all Internet-bound requests, in order to identify prohibited activities and assist incident handlers with identifying potentially compromised systems?	8
Continuous Monitoring	Deactivated Account Activity	MON-01.10	Mechanisms exist to monitor deactivated accounts for attempted usage.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Security Incident Event Manager (SIEM) - Splunk - NNT Change Tracker		Does the organization monitor deactivated accounts for attempted usage?	9
Continuous Monitoring	Automated Response to Suspicious Events	MON-01.11	Mechanisms exist to automatically implement pre-determined corrective actions in response to detected events that have security incident implications.			Does the organization alert incident response personnel of detected suspicious events and implement actions to terminate suspicious events?	5
Continuous Monitoring	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.			Does the organization alert incident response personnel of inappropriate or unusual activities that have security incident implications?	5
Continuous Monitoring	Alert Threshold Tuning	MON-01.13	Mechanisms exist to "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events.			Does the organization "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events?	5
Continuous Monitoring	Individuals Posing Greater Risk	MON-01.14	Mechanisms exist to implement enhanced activity monitoring for individuals who have been identified as posing an increased level of risk.		E-MON-03	Does the organization implement enhanced activity monitoring for individuals who have been identified as posing an increased level of risk?	5
Continuous Monitoring	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.		E-MON-03	Does the organization implement enhanced activity monitoring for privileged users?	5
Continuous Monitoring	Analyze and Prioritize Monitoring Requirements	MON-01.16	Mechanisms exist to assess the organization's needs for monitoring and prioritize the monitoring of assets, based on asset criticality and the sensitivity of the data it stores, transmits and processes.			Does the organization assess the organization's needs for monitoring and prioritize the monitoring of assets, based on asset criticality and the sensitivity of the data it stores, transmits and processes?	5

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Continuous Monitoring	Real-Time Session Monitoring	MON-01.17	Mechanisms exist to enable authorized personnel the ability to remotely view and hear content related to an established user session in real time, in accordance with organizational standards, as well as statutory, regulatory and contractual obligations.			Does the organization enable authorized personnel the ability to remotely view and hear content related to an established user session in real time?	4
Continuous Monitoring	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.	- Security Incident Event Manager (SIEM) - Splunk	E-MON-01 E-MON-05	Does the organization utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs?	10
Continuous Monitoring	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.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Security Incident Event Manager (SIEM) - Splunk - NNT Change Tracker		Does the organization use automated mechanisms to correlate logs from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to maintain situational awareness?	9
Continuous Monitoring	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)	E-MON-01 E-MON-02 E-MON-05	Does the organization centrally collect, review and analyze audit records from multiple sources?	5
Continuous Monitoring	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.			Does the organization 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
Continuous Monitoring	Correlation with Physical Monitoring	MON-02.4	Automated mechanisms exist to correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual or malevolent activity.			Does the organization correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual or malevolent activity?	5
Continuous Monitoring	Permitted Actions	MON-02.5	Mechanisms exist to specify the permitted actions for both users and systems associated with the review, analysis and reporting of audit information.			Does the organization specify the permitted actions for both users and systems associated with the review, analysis and reporting of audit information?	5
Continuous Monitoring	Audit Level Adjustments	MON-02.6	Mechanisms exist to adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence.			Does the organization adjust the level of audit review, analysis and reporting based on evolving threat information from law enforcement, industry associations or other credible sources of threat intelligence?	5
Continuous Monitoring	System-Wide / Time-Correlated Audit Trail	MON-02.7	Automated mechanisms exist to compile audit records into an organization-wide audit trail that is time-correlated.			Does the organization compile audit records into an organization-wide audit trail that is time-correlated?	5
Continuous Monitoring	Changes by Authorized Individuals	MON-02.8	Mechanisms exist to provide privileged users or roles the capability to change the auditing to be performed on specified information system components, based on specific event criteria within specified time thresholds.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization provide privileged users or roles the capability to change the auditing to be performed on specified information system components, based on specific event criteria within specified time thresholds?	5
Continuous Monitoring	Content of Event Logs	MON-03	Mechanisms exist to configure systems to produce audit records that contain sufficient information to, at a minimum: • Establish what type of event occurred; • When (date and time) the event occurred; • Where the event occurred;	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization configure systems to produce audit records that contain sufficient information to, at a minimum: • Establish what type of event occurred; • When (date and time) the event occurred; • Where the event occurred;	10
Continuous Monitoring	Sensitive Audit Information	MON-03.1	Mechanisms exist to protect sensitive/regulated data contained in log files.			Does the organization protect sensitive/regulated data contained in log files?	8
Continuous Monitoring	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.			Does the organization link system access to individual users or service accounts?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Continuous Monitoring	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	- Security Incident Event Manager (SIEM) - Splunk		Does the organization log and review the actions of users and/or services with elevated privileges?	8
Continuous Monitoring	Verbosity Logging for Boundary Devices	MON-03.4	Mechanisms exist to verbosely log all traffic (both allowed and blocked) arriving at network boundary devices, including firewalls, Intrusion Detection / Prevention Systems (IDS/IPS) and inbound and outbound proxies.			Does the organization verbosely log all traffic (both allowed and blocked) arriving at network boundary devices, including firewalls, Intrusion Detection / Prevention Systems (IDS/IPS) and inbound and outbound proxies?	5
Continuous Monitoring	Limit Personal Data (PD) In Audit Records	MON-03.5	Mechanisms exist to limit Personal Data (PD) contained in audit records to the elements identified in the privacy risk assessment.	- Data Protection Impact Assessment (DPIA)		Does the organization limit Personal Data (PD) contained in audit records to the elements identified in the privacy risk assessment?	8
Continuous Monitoring	Centralized Management of Planned Audit Record Content	MON-03.6	Mechanisms exist to centrally manage and configure the content required to be captured in audit records generated by organization-defined information system components.			Does the organization centrally manage and configure the content required to be captured in audit records generated by organization-defined information system components?	5
Continuous Monitoring	Database Logging	MON-03.7	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.			Does the organization ensure databases produce audit records that contain sufficient information to monitor database activities that includes, at a minimum: ▪ Access to particularly important information; ▪ Addition of new users, especially privileged users; ▪ Any query containing comments;	8
Continuous Monitoring	Event Log Storage Capacity	MON-04	Mechanisms exist to allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded.			Does the organization allocate and proactively manage sufficient event log storage capacity to reduce the likelihood of such capacity being exceeded?	8
Continuous Monitoring	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.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Security Incident Event Manager (SIEM) - Splunk - NNT Change Tracker		Does the organization alert appropriate personnel in the event of a log processing failure and take actions to remedy the disruption?	8
Continuous Monitoring	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Security Incident Event Manager (SIEM) - Splunk - NNT Change Tracker		Does the organization provide 24x7x365 near real-time alerting capability when an event log processing failure occurs?	6
Continuous Monitoring	Event Log Storage Capacity Alerting	MON-05.2	Automated mechanisms exist to alert appropriate personnel when the allocated volume reaches an organization-defined percentage of maximum event log storage capacity.			Does the organization alert appropriate personnel when the allocated volume reaches an organization-defined percentage of maximum event log storage capacity?	5
Continuous Monitoring	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Security Incident Event Manager (SIEM) - Splunk - NNT Change Tracker		Does the organization provide an event log report generation capability to aid in detecting and assessing anomalous activities?	7
Continuous Monitoring	Query Parameter Audits of Personal Data (PD)	MON-06.1	Mechanisms exist to provide and implement the capability for auditing the parameters of user query events for data sets containing Personal Data (PD).			Does the organization provide and implement the capability for auditing the parameters of user query events for data sets containing Personal Data (PD)?	3
Continuous Monitoring	Trend Analysis Reporting	MON-06.2	Mechanisms exist to employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data.			Does the organization employ trend analyses to determine if security control implementations, the frequency of continuous monitoring activities, and/or the types of activities used in the continuous monitoring process need to be modified based on empirical data?	5
Continuous Monitoring	Time Stamps	MON-07	Mechanisms exist to configure systems to use an authoritative time source to generate time stamps for event logs.			Does the organization configure systems to use an authoritative time source to generate time stamps for event logs?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Continuous Monitoring	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	- Network Time Protocol (NTP)		Does the organization synchronize internal system clocks with an authoritative time source?	8
Continuous Monitoring	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Security Incident Event Manager (SIEM) - Splunk		Does the organization protect event logs and audit tools from unauthorized access, modification and deletion?	10
Continuous Monitoring	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.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Security Incident Event Manager (SIEM) - Splunk		Does the organization back up event logs onto a physically different system or system component than the Security Incident Event Manager (SIEM) or similar automated tool?	5
Continuous Monitoring	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.	- Security Incident Event Manager (SIEM) - Splunk		Does the organization restrict access to the management of event logs to privileged users with a specific business need?	8
Continuous Monitoring	Cryptographic Protection of Event Log Information	MON-08.3	Cryptographic mechanisms exist to protect the integrity of event logs and audit tools.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization protect the integrity of event logs and audit tools with cryptographic mechanisms?	5
Continuous Monitoring	Dual Authorization for Event Log Movement	MON-08.4	Automated mechanisms exist to enforce dual authorization for the movement or deletion of event logs.			Does the organization enforce dual authorization for the movement or deletion of event logs?	5
Continuous Monitoring	Non-Repudiation	MON-09	Mechanisms exist to utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization utilize a non-repudiation capability to protect against an individual falsely denying having performed a particular action?	8
Continuous Monitoring	Identity Binding	MON-09.1	Mechanisms exist to bind the identity of the information producer to the information generated.			Does the organization bind the identity of the information producer to the information generated?	4
Continuous Monitoring	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.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)	E-AST-11	Does the organization 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?	10
Continuous Monitoring	Monitoring For Information Disclosure	MON-11	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of non-public information.	- Content filtering solution - Review of social media outlets		Does the organization monitor for evidence of unauthorized exfiltration or disclosure of non-public information?	8
Continuous Monitoring	Analyze Traffic for Covert Exfiltration	MON-11.1	Automated mechanisms exist to analyze network traffic to detect covert data exfiltration.			Does the organization analyze network traffic to detect covert data exfiltration?	5
Continuous Monitoring	Unauthorized Network Services	MON-11.2	Automated mechanisms exist to detect unauthorized network services and alert incident response personnel.			Does the organization detect unauthorized network services and alert incident response personnel?	5
Continuous Monitoring	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization identify and alert on Indicators of Compromise (IoC)?	5

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Continuous Monitoring	Session Audit	MON-12	Mechanisms exist to provide session audit capabilities that can: • Capture and log all content related to a user session; and • Remotely view all content related to an established user session in real time.	- NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization provide session audit capabilities that: • Capture and log all content related to a user session; and • Remotely view all content related to an established user session in real time?	7
Continuous Monitoring	Alternate Event Logging Capability	MON-13	Mechanisms exist to provide an alternate event logging capability in the event of a failure in primary audit capability.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization provide an alternate audit capability in the event of a failure in primary audit capability?	3
Continuous Monitoring	Cross-Organizational Monitoring	MON-14	Mechanisms exist to coordinate sanitized event logs among external organizations to identify anomalous events when event logs are shared across organizational boundaries, without giving away sensitive or critical business data.			Does the organization coordinate sanitized event logs among external organizations to identify anomalous events when event logs are shared across organizational boundaries, without giving away sensitive or critical business data?	3
Continuous Monitoring	Sharing of Event Logs	MON-14.1	Mechanisms exist to share event logs with third-party organizations based on specific cross-organizational sharing agreements.	- Veris (incident sharing) (http://veriscommunity.net)		Does the organization share event logs with third-party organizations based on specific cross-organizational sharing agreements?	5
Continuous Monitoring	Covert Channel Analysis	MON-15	Mechanisms exist to conduct covert channel analysis to identify aspects of communications that are potential avenues for covert channels.			Does the organization conduct covert channel analysis to identify aspects of communications that are potential avenues for covert channels?	3
Continuous Monitoring	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization detect and respond to anomalous behavior that could indicate account compromise or other malicious activities?	10
Continuous Monitoring	Insider Threats	MON-16.1	Mechanisms exist to monitor internal personnel activity for potential security incidents.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization monitor internal personnel activity for potential security incidents?	8
Continuous Monitoring	Third-Party Threats	MON-16.2	Mechanisms exist to monitor third-party personnel activity for potential security incidents.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization monitor third-party personnel activity for potential security incidents?	8
Continuous Monitoring	Unauthorized Activities	MON-16.3	Mechanisms exist to monitor for unauthorized activities, accounts, connections, devices and software.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization monitor for unauthorized activities, accounts, connections, devices and software?	8
Continuous Monitoring	Account Creation and Modification Logging	MON-16.4	Automated mechanisms exist to generate event logs for permissions changes to privileged accounts and/or groups.			Does the organization ensure event logs are generated for permissions changes to privileged accounts and/or groups.	7
Cryptographic Protections	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	- Key and certificate management solutions - Microsoft BitLocker (https://www.microsoft.com/en-us/download/details.aspx?id=53006) - Symantec Endpoint Encryption (https://www.symantec.com/products/endpoint-protection)		Does the organization facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies?	10
Cryptographic Protections	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.			Are cryptographic mechanisms used to prevent unauthorized disclosure of information as an alternative to physical safeguards?	5
Cryptographic Protections	Export-Controlled Technology	CRY-01.2	Mechanisms exist to address the exporting of cryptographic technologies in compliance with relevant statutory and regulatory requirements.			Does the organization address the exporting of cryptographic technologies in compliance with relevant statutory and regulatory requirements?	5

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Cryptographic Protections	Pre/Post Transmission Handling	CRY-01.3	Cryptographic mechanisms exist to ensure the confidentiality and integrity of information during preparation for transmission and during reception.			Does the organization ensure the confidentiality and integrity of information during preparation for transmission and during reception with cryptographic mechanisms?	5
Cryptographic Protections	Conceal / Randomize Communications	CRY-01.4	Cryptographic mechanisms exist to conceal or randomize communication patterns.			Does the organization conceal or randomize communication patterns with cryptographic mechanisms?	5
Cryptographic Protections	Cryptographic Cipher Suites and Protocols Inventory	CRY-01.5	Mechanisms exist to identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols.			Does the organization identify, document and review deployed cryptographic cipher suites and protocols to proactively respond to industry trends regarding the continued viability of utilized cryptographic cipher suites and protocols?	9
Cryptographic Protections	Cryptographic Module Authentication	CRY-02	Automated mechanisms exist to enable systems to authenticate to a cryptographic module.	- Yubico (https://www.yubico.com)		Do cryptographic mechanisms authenticate to a cryptographic module?	8
Cryptographic Protections	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	- SSL / TLS protocols - IPSEC Tunnels - Native MPLS encrypted tunnel configurations - Custom encrypted payloads	E-CRY-01	Are cryptographic mechanisms utilized to protect the confidentiality of data being transmitted?	10
Cryptographic Protections	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.		E-CRY-01	Are cryptographic mechanisms utilized to protect the integrity of data being transmitted?	10
Cryptographic Protections	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	- Symantec Endpoint Encryption (https://www.symantec.com/products/endpoint-protection)		Are cryptographic mechanisms utilized on systems to prevent unauthorized disclosure of data at rest?	10
Cryptographic Protections	Storage Media	CRY-05.1	Cryptographic mechanisms exist to protect the confidentiality and integrity of sensitive/regulated data residing on storage media.	- Native Storage Area Network (SAN) encryption functionality - BitLocker and EFS		Are cryptographic mechanisms utilized to protect the confidentiality and integrity of sensitive/regulated data residing on storage media?	8
Cryptographic Protections	Offline Storage	CRY-05.2	Mechanisms exist to remove unused data from online storage and archive it off-line in a secure location until it can be disposed of according to data retention requirements.			Does the organization remove unused data from online storage and archive it off-line in a secure location until it can be disposed of according to data retention requirements?	5
Cryptographic Protections	Database Encryption	CRY-05.3	Mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.			Does the organization ensure the hard disks of database servers are encrypted using Full Disk Encryption (FDE)?	8
Cryptographic Protections	Non-Console Administrative Access	CRY-06	Cryptographic mechanisms exist to protect the confidentiality and integrity of non-console administrative access.			Are cryptographic mechanisms used to protect the confidentiality and integrity of non-console administrative access?	9
Cryptographic Protections	Wireless Access Authentication & Encryption	CRY-07	Mechanisms exist to protect wireless access via secure authentication and encryption.			Does the organization protect wireless access via secure authentication and encryption?	9
Cryptographic Protections	Public Key Infrastructure (PKI)	CRY-08	Mechanisms exist to securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.	- Microsoft Active Directory (AD) Certificate Services - Digitcert (https://www.digicert.com) - Entrust (https://www.entrust.com) - Comodo (https://www.comodo.com) - Vault (https://www.vaultproject.io/)		Does the organization securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Cryptographic Protections	Availability	CRY-08.1	Resiliency mechanisms exist to ensure the availability of data in the event of the loss of cryptographic keys.			Does the organization have appropriate resiliency mechanisms to ensure the availability of data in the event of the loss of cryptographic keys?	9
Cryptographic Protections	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	- Microsoft Active Directory (AD) Certificate Services - Digitcert (https://www.digicert.com) - Entrust (https://www.entrust.com) - Comodo (https://www.comodo.com) - Vault (https://www.vaultproject.io/)	E-CRY-01	Does the organization facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys?	10
Cryptographic Protections	Symmetric Keys	CRY-09.1	Mechanisms exist to facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes.		E-CRY-01	Does the organization facilitate the production and management of symmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes?	9
Cryptographic Protections	Asymmetric Keys	CRY-09.2	Mechanisms exist to facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes that protect the user's private key.		E-CRY-01	Does the organization facilitate the production and management of asymmetric cryptographic keys using Federal Information Processing Standards (FIPS)-compliant key management technology and processes that protect the user's private key?	9
Cryptographic Protections	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	- Escrowing of encryption keys is a common practice for ensuring availability in the event of loss of keys.		Does the organization ensure the availability of information in the event of the loss of cryptographic keys by individual users?	8
Cryptographic Protections	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.			Does the organization facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes?	9
Cryptographic Protections	Assigned Owners	CRY-09.5	Mechanisms exist to ensure cryptographic keys are bound to individual identities.			Does the organization ensure cryptographic keys are bound to individual identities?	8
Cryptographic Protections	Third-Party Cryptographic Keys	CRY-09.6	Mechanisms exist to ensure customers are provided with appropriate key management guidance whenever cryptographic keys are shared.			Does the organization ensure customers are provided with appropriate key management guidance whenever cryptographic keys are shared?	7
Cryptographic Protections	External System Cryptographic Key Control	CRY-09.7	Mechanisms exist to maintain control of cryptographic keys for encrypted material stored or transmitted through an external system.			Does the organization maintain control of cryptographic keys for encrypted material stored or transmitted through an external system?	5
Cryptographic Protections	Transmission of Security & Privacy Attributes	CRY-10	Mechanisms exist to ensure systems associate security attributes with information exchanged between systems.	- Integrity checking		Does the organization ensure systems associate security attributes with information exchanged between systems?	5
Cryptographic Protections	Certificate Authorities	CRY-11	Automated mechanisms exist to enable the use of organization-defined Certificate Authorities (CAs) to facilitate the establishment of protected sessions.			Does the organization enable the use of organization-defined Certificate Authorities (CAs) to facilitate the establishment of protected sessions?	8
Data Classification & Handling	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.			Does the organization facilitate the implementation of data protection controls?	10
Data Classification & Handling	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.			Does the organization ensure data stewardship is assigned, documented and communicated?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Data Classification & Handling	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.			Does the organization protect sensitive/regulated data wherever it is stored?	9
Data Classification & Handling	Sensitive / Regulated Media Records	DCH-01.3	Mechanisms exist to ensure media records for sensitive/regulated data contain sufficient information to determine the potential impact in the event of a data loss incident.			Does the organization ensure media records for sensitive/regulated data contain sufficient information to determine the potential impact in the event of a data loss incident?	6
Data Classification & Handling	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.		E-DCH-01 E-DCH-02	Does the organization ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements?	10
Data Classification & Handling	Highest Classification Level	DCH-02.1	Mechanisms exist to ensure that systems, applications and services are classified according to the highest level of data sensitivity that is stored, transmitted and/or processed.			Does the organization ensure that systems, applications and services are classified according to the highest level of data sensitivity that is stored, transmitted and/or processed?	8
Data Classification & Handling	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	- Data Loss Prevention (DLP)		Does the organization control and restrict access to digital and non-digital media to authorized individuals?	8
Data Classification & Handling	Disclosure of Information	DCH-03.1	Mechanisms exist to restrict the disclosure of sensitive / regulated data to authorized parties with a need to know.			Does the organization limit the disclosure of data to authorized parties?	10
Data Classification & Handling	Masking Displayed Data	DCH-03.2	Mechanisms exist to apply data masking to sensitive information that is displayed or printed.			Does the organization apply data masking to sensitive information that is displayed or printed?	7
Data Classification & Handling	Controlled Release	DCH-03.3	Automated mechanisms exist to validate cybersecurity and privacy attributes prior to releasing information to external systems.			Does the organization automatically validate cybersecurity and privacy attributes prior to releasing information to external systems?	4
Data Classification & Handling	Media Marking	DCH-04	Mechanisms exist to mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements.			Does the organization mark media in accordance with data protection requirements so that personnel are alerted to distribution limitations, handling caveats and applicable security requirements?	7
Data Classification & Handling	Automated Marking	DCH-04.1	Automated mechanisms exist to mark physical media and digital files to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies.			Does the organization use automated mechanisms to mark media and system output to indicate the distribution limitations, handling requirements and applicable security markings (if any) of the information to aid Data Loss Prevention (DLP) technologies?	2
Data Classification & Handling	Security & Privacy Attributes	DCH-05	Mechanisms exist to bind security attributes to information as it is stored, transmitted and processed.			Does the organization bind security attributes to information as it is stored, transmitted and processed?	2
Data Classification & Handling	Dynamic Attribute Association	DCH-05.1	Mechanisms exist to dynamically associate cybersecurity and privacy attributes with individuals and objects as information is created, combined, or transformed, in accordance with organization-defined cybersecurity and privacy policies.			Does the organization dynamically associate cybersecurity and privacy attributes with individuals and objects as information is created, combined, or transformed, in accordance with organization-defined cybersecurity and privacy policies?	2
Data Classification & Handling	Attribute Value Changes By Authorized Individuals	DCH-05.2	Mechanisms exist to provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated cybersecurity and privacy attributes.			Does the organization provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated cybersecurity and privacy attributes?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Data Classification & Handling	Maintenance of Attribute Associations By System	DCH-05.3	Mechanisms exist to maintain the association and integrity of cybersecurity and privacy attributes to individuals and objects.			Does the organization maintain the association and integrity of cybersecurity and privacy attributes to individuals and objects?	2
Data Classification & Handling	Association of Attributes By Authorized Individuals	DCH-05.4	Mechanisms exist to provide the capability to associate cybersecurity and privacy attributes with individuals and objects by authorized individuals (or processes acting on behalf of individuals).			Does the organization provide the capability to associate cybersecurity and privacy attributes with individuals and objects by authorized individuals (or processes acting on behalf of individuals)?	2
Data Classification & Handling	Attribute Displays for Output Devices	DCH-05.5	Mechanisms exist to display cybersecurity and privacy attributes in human-readable form on each object that the system transmits to output devices to identify special dissemination, handling or distribution instructions using human-readable, standard naming conventions.			Does the organization display cybersecurity and privacy attributes in human-readable form on each object that the system transmits to output devices to identify special dissemination, handling or distribution instructions using human-readable, standard naming conventions?	8
Data Classification & Handling	Data Subject Attribute Associations	DCH-05.6	Mechanisms exist to require personnel to associate and maintain the association of cybersecurity and privacy attributes with individuals and objects in accordance with cybersecurity and privacy policies.			Does the organization require personnel to associate and maintain the association of cybersecurity and privacy attributes with individuals and objects in accordance with cybersecurity and privacy policies?	2
Data Classification & Handling	Consistent Attribute Interpretation	DCH-05.7	Mechanisms exist to provide a consistent, organizationally agreed upon interpretation of cybersecurity and privacy attributes employed in access enforcement and flow enforcement decisions between distributed system components.			Does the organization provide a provide a consistent, organizationally agreed upon interpretation of cybersecurity and privacy attributes employed in access enforcement and flow enforcement decisions between distributed system components?	2
Data Classification & Handling	Identity Association Techniques & Technologies	DCH-05.8	Mechanisms exist to associate cybersecurity and privacy attributes to information.			Does the organization associate cybersecurity and privacy attributes to information?	2
Data Classification & Handling	Attribute Reassignment	DCH-05.9	Mechanisms exist to reclassify data as required, due to changing business/technical requirements.			Does the organization reclassify data as required, due to changing business/technical requirements?	7
Data Classification & Handling	Attribute Configuration By Authorized Individuals	DCH-05.10	Mechanisms exist to provide authorized individuals the capability to define or change the type and value of cybersecurity and privacy attributes available for association with subjects and objects.			Does the organization provide authorized individuals the capability to define or change the type and value of cybersecurity and privacy attributes available for association with subjects and objects?	8
Data Classification & Handling	Audit Changes	DCH-05.11	Mechanisms exist to audit changes to cybersecurity and privacy attributes and responds to events in accordance with incident response procedures.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization audit changes to cybersecurity and privacy attributes and respond to them in a timely manner?	7
Data Classification & Handling	Media Storage	DCH-06	Mechanisms exist to: • Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and • Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.			Does the organization: • Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and • Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures?	8
Data Classification & Handling	Physically Secure All Media	DCH-06.1	Mechanisms exist to physically secure all media that contains sensitive information.	- Lockbox		Does the organization physically secure all media that contains sensitive information?	9
Data Classification & Handling	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.		E-AST-08	Does the organization maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually?	9
Data Classification & Handling	Periodic Scans for Sensitive Data	DCH-06.3	Mechanisms exist to periodically scan unstructured data sources for sensitive/regulated data or data requiring special protection measures by statutory, regulatory or contractual obligations.			Does the organization periodically scan unstructured data sources for sensitive/regulated data or data requiring special protection measures by statutory, regulatory or contractual obligations?	7

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Data Classification & Handling	Making Sensitive Data Unreadable In Storage	DCH-06.4	Mechanisms exist to ensure sensitive/regulated data is rendered human unreadable anywhere sensitive/regulated data is stored.			Does the organization ensure sensitive/regulated data is rendered human unreadable anywhere sensitive/regulated data is stored?	9
Data Classification & Handling	Storing Authentication Data	DCH-06.5	Mechanisms exist to prohibit the storage of sensitive transaction authentication data after authorization.			Does the organization prohibit the storage of sensitive authentication data after authorization?	5
Data Classification & Handling	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	- Assigned couriers		Does the organization protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures?	9
Data Classification & Handling	Custodians	DCH-07.1	Mechanisms exist to identify custodians throughout the transport of digital or non-digital media.	- Chain of custody		Does the organization identify custodians throughout the transport of digital or non-digital media?	9
Data Classification & Handling	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.			Does the organization protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas with cryptographic mechanisms?	5
Data Classification & Handling	Physical Media Disposal	DCH-08	Mechanisms exist to securely dispose of media when it is no longer required, using formal procedures.	- Shred-it - IronMountain - DoD-strength data erasers	E-AST-03	Does the organization securely dispose of media when it is no longer required, using formal procedures?	10
Data Classification & Handling	Digital Media Sanitization	DCH-09	Mechanisms exist to sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.		E-AST-03 E-DCH-07	Does the organization sanitize digital media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse?	10
Data Classification & Handling	Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify media sanitization and disposal actions.	- Certificate of destruction	E-AST-03 E-DCH-07	Does the organization supervise, track, document and verify media sanitization and disposal actions?	7
Data Classification & Handling	Equipment Testing	DCH-09.2	Mechanisms exist to test sanitization equipment and procedures to verify that the intended result is achieved.			Does the organization test sanitization equipment and procedures to verify that the intended result is achieved?	5
Data Classification & Handling	Sanitization of Personal Data (PD)	DCH-09.3	Mechanisms exist to facilitate the sanitization of Personal Data (PD).	- De-identifying PI		Does the organization facilitate the sanitization of Personal Data (PD)?	9
Data Classification & Handling	First Time Use Sanitization	DCH-09.4	Mechanisms exist to apply nondestructive sanitization techniques to portable storage devices prior to first use.			Does the organization apply nondestructive sanitization techniques to portable storage devices prior to first use?	5
Data Classification & Handling	Dual Authorization for Sensitive Data Destruction	DCH-09.5	Mechanisms exist to enforce dual authorization for the destruction, disposal or sanitization of digital media that contains sensitive / regulated data.			Does the organization enforce dual authorization for the destruction, disposal or sanitization of digital media that contains sensitive/regulated data?	5
Data Classification & Handling	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.			Does the organization restrict the use of types of digital media on systems or system components?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Data Classification & Handling	Limitations on Use	DCH-10.1	Mechanisms exist to restrict the use and distribution of sensitive / regulated data.			Does the organization restrict the use and distribution of sensitive/regulated data?	10
Data Classification & Handling	Prohibit Use Without Owner	DCH-10.2	Mechanisms exist to prohibit the use of portable storage devices in organizational information systems when such devices have no identifiable owner.			Does the organization prohibit the use of portable storage devices in organizational information systems when such devices have no identifiable owner?	5
Data Classification & Handling	Data Reclassification	DCH-11	Mechanisms exist to reclassify data, including associated systems, applications and services, commensurate with the security category and/or classification level of the information.			Does the organization reclassify data, including associated systems, applications and services, commensurate with the security category and/or classification level of the information?	8
Data Classification & Handling	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.			Does the organization restrict removable media in accordance with data handling and acceptable usage parameters?	10
Data Classification & Handling	Use of External Information Systems	DCH-13	Mechanisms exist to govern how external parties, systems and services are used to securely store, process and transmit data.			Does the organization govern how external parties, systems and services are used to securely store, process and transmit data?	9
Data Classification & Handling	Limits of Authorized Use	DCH-13.1	Mechanisms exist to prohibit external parties, systems and services from storing, processing and transmitting data unless authorized individuals first: • Verifying the implementation of required security controls; or • Retaining a processing agreement with the entity hosting the external systems or service.			Does the organization prohibit external parties, systems and services from storing, processing and transmitting data unless authorized individuals first: ▪ Verifying the implementation of required security controls; or ▪ Retaining a processing agreement with the entity hosting the external systems or service?	8
Data Classification & Handling	Portable Storage Devices	DCH-13.2	Mechanisms exist to restrict or prohibit the use of portable storage devices by users on external systems.			Does the organization restrict or prohibit the use of portable storage devices by users on external systems?	9
Data Classification & Handling	Protecting Sensitive Data on External Systems	DCH-13.3	Mechanisms exist to ensure that the requirements for the protection of sensitive information processed, stored or transmitted on external systems, are implemented in accordance with applicable statutory, regulatory and contractual obligations.	- NIST 800-171 Compliance Criteria (NCC) (ComplianceForge)		Does the organization ensure that the requirements for the protection of sensitive information processed, stored or transmitted on external systems, are implemented in accordance with applicable statutory, regulatory and contractual obligations?	10
Data Classification & Handling	Non-Organizationally Owned Systems / Components / Devices	DCH-13.4	Mechanisms exist to restrict the use of non-organizationally owned information systems, system components or devices to process, store or transmit organizational information.			Does the organization restrict the use of non-organizationally owned information systems, system components or devices to process, store or transmit organizational information?	5
Data Classification & Handling	Information Sharing	DCH-14	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	- ShareFile - SmartVault - Veris (incident sharing) (http://veriscommunity.net)		Does the organization utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected?	9
Data Classification & Handling	Information Search & Retrieval	DCH-14.1	Mechanisms exist to ensure information systems implement data search and retrieval functions that properly enforce data protection / sharing restrictions.			Does the organization ensure information systems implement data search and retrieval functions that properly enforce data protection / sharing restrictions?	5
Data Classification & Handling	Transfer Authorizations	DCH-14.2	Mechanisms exist to verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (e.g., write permissions or privileges) prior to transferring said data.			Does the organization verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (e.g., write permissions or privileges) prior to accepting such data?	8
Data Classification & Handling	Data Access Mapping	DCH-14.3	Mechanisms exist to develop a data-specific Access Control List (ACL) or Data Information Sharing Agreement (DISA) to determine the personnel with whom sensitive/regulated data is shared.			Does the organization develop a data-specific Access Control List (ACL) or Data Information Sharing Agreement (DISA) to determine the personnel with whom sensitive/regulated data is shared?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Data Classification & Handling	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	- Designate individuals authorized to post information onto systems that are publicly accessible. - Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.		Does the organization control publicly-accessible content?	10
Data Classification & Handling	Data Mining Protection	DCH-16	Mechanisms exist to protect data storage objects against unauthorized data mining and data harvesting techniques.			Does the organization protect data storage objects against unauthorized data mining and data harvesting techniques?	7
Data Classification & Handling	Ad-Hoc Transfers	DCH-17	Mechanisms exist to secure ad-hoc exchanges of large digital files with internal or external parties.	- ShareFile - Box		Does the organization secure ad-hoc exchanges of large digital files with internal or external parties?	8
Data Classification & Handling	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	- Data Protection Impact Assessment (DPIA)	E-AST-11	Does the organization retain media and data in accordance with applicable statutory, regulatory and contractual obligations?	8
Data Classification & Handling	Minimize Personal Data (PD)	DCH-18.1	Mechanisms exist to limit Personal Data (PD) being processed in the information lifecycle to elements identified in the Data Protection Impact Assessment (DPIA).	- Data Protection Impact Assessment (DPIA)		Does the organization limit Personal Data (PD) being processed in the information lifecycle to elements identified in the Data Protection Impact Assessment (DPIA)?	8
Data Classification & Handling	Limit Personal Data (PD) Elements In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of Personal Data (PD) for research, testing, or training, in accordance with the Data Protection Impact Assessment (DPIA).	- Data Protection Impact Assessment (DPIA)		Does the organization minimize the use of Personal Data (PD) for research, testing, or training, in accordance with the Data Protection Impact Assessment (DPIA)?	8
Data Classification & Handling	Temporary Files Containing Personal Data (PD)	DCH-18.3	Mechanisms exist to perform periodic checks of temporary files for the existence of Personal Data (PD).			Does the organization perform periodic checks of temporary files for the existence of Personal Data (PD)?	5
Data Classification & Handling	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.		E-AST-23	Does the organization inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties?	9
Data Classification & Handling	Archived Data Sets	DCH-20	Mechanisms exist to protect archived data in accordance with applicable statutory, regulatory and contractual obligations.			Does the organization protect archived data in accordance with applicable statutory, regulatory and contractual obligations?	8
Data Classification & Handling	Information Disposal	DCH-21	Mechanisms exist to securely dispose of, destroy or erase information.	- Shred-it - IronMountain		Does the organization securely dispose of, destroy or erase information?	10
Data Classification & Handling	Data Quality Operations	DCH-22	Mechanisms exist to check for the accuracy, relevance, timeliness, impact, completeness and de-identification of information across the information lifecycle.	- Data Protection Impact Assessment (DPIA)		Does the organization check for the accuracy, relevance, timeliness, impact, completeness and de-identification of information across the information lifecycle?	5
Data Classification & Handling	Updating & Correcting Personal Data (PD)	DCH-22.1	Mechanisms exist to utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified.	- Data Protection Impact Assessment (DPIA)		Does the organization utilize technical controls to correct Personal Data (PD) that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified?	6
Data Classification & Handling	Data Tags	DCH-22.2	Mechanisms exist to utilize data tags to automate tracking of sensitive/regulated data across the information lifecycle.	- Data Protection Impact Assessment (DPIA)		Does the organization utilize data tags to automate tracking of Personal Data (PD) across the information lifecycle?	3

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Data Classification & Handling	Primary Source Personal Data (PD) Collection	DCH-22.3	Mechanisms exist to collect Personal Data (PD) directly from the individual.	- Data Protection Impact Assessment (DPIA)		Does the organization collect Personal Data (PD) directly from the individual?	8
Data Classification & Handling	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	- Data Protection Impact Assessment (DPIA)		Does the organization remove Personal Data (PD) from datasets?	8
Data Classification & Handling	De-Identify Dataset Upon Collection	DCH-23.1	Mechanisms exist to de-identify the dataset upon collection by not collecting Personal Data (PD).	- Data Protection Impact Assessment (DPIA)		Does the organization de-identify the dataset upon collection by not collecting Personal Data (PD)?	8
Data Classification & Handling	Archiving	DCH-23.2	Mechanisms exist to refrain from archiving Personal Data (PD) elements if those elements in a dataset will not be needed after the dataset is archived.	- Data Protection Impact Assessment (DPIA)		Does the organization refrain from archiving Personal Data (PD) elements if those elements in a dataset will not be needed after the dataset is archived?	8
Data Classification & Handling	Release	DCH-23.3	Mechanisms exist to remove Personal Data (PD) elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.	- Data Protection Impact Assessment (DPIA)		Does the organization remove Personal Data (PD) elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release?	8
Data Classification & Handling	Removal, Masking, Encryption, Hashing or Replacement of Direct Identifiers	DCH-23.4	Mechanisms exist to remove, mask, encrypt, hash or replace direct identifiers in a dataset.	- Data Protection Impact Assessment (DPIA)		Does the organization remove, mask, encrypt, hash or replace direct identifiers in a dataset?	8
Data Classification & Handling	Statistical Disclosure Control	DCH-23.5	Mechanisms exist to manipulate numerical data, contingency tables and statistical findings so that no person or organization is identifiable in the results of the analysis.			Does the organization manipulate numerical data, contingency tables and statistical findings so that no person or organization is identifiable in the results of the analysis?	1
Data Classification & Handling	Differential Privacy	DCH-23.6	Mechanisms exist to prevent disclosure of Personal Data (PD) by adding non-deterministic noise to the results of mathematical operations before the results are reported.	- Data Protection Impact Assessment (DPIA)		Does the organization prevent disclosure of Personal Data (PD) by adding non-deterministic noise to the results of mathematical operations before the results are reported?	1
Data Classification & Handling	Automated De-Identification of Sensitive Data	DCH-23.7	Mechanisms exist to perform de-identification of sensitive/regulated data, using validated algorithms and software to implement the algorithms.	- Data Protection Impact Assessment (DPIA)		Does the organization perform de-identification using validated algorithms and software to implement the algorithms?	1
Data Classification & Handling	Motivated Intruder	DCH-23.8	Mechanisms exist to perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.			Does the organization perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified?	3
Data Classification & Handling	Code Names	DCH-23.9	Mechanisms exist to use aliases to name assets, which are mission-critical and/or contain highly-sensitive/regulated data, are unique and not readily associated with a product, project or type of data.			Does the organization use aliases to name assets, which are mission-critical and/or contain highly-sensitive/regulated data, are unique and not readily associated with a product, project or type of data?	1
Data Classification & Handling	Information Location	DCH-24	Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.	- Data Flow Diagram (DFD)	E-AST-23	Does the organization identify and document the location of information and the specific system components on which the information resides?	10
Data Classification & Handling	Automated Tools to Support Information Location	DCH-24.1	Automated mechanisms exist to identify by data classification type to ensure adequate cybersecurity and privacy controls are in place to protect organizational information and individual privacy.			Does the organization use automated mechanisms to identify by data classification type to ensure adequate cybersecurity and privacy controls are in place to protect organizational information and individual privacy?	6

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Data Classification & Handling	Transfer of Sensitive and/or Regulated Data	DCH-25	Mechanisms exist to restrict and govern the transfer of sensitive and/or regulated data to third-countries or international organizations.	- Model contracts - Privacy Shield - Binding Corporate Rules (BCR)		Does the organization restrict and govern the transfer of data to third-countries or international organizations?	10
Data Classification & Handling	Transfer Activity Limits	DCH-25.1	Mechanisms exist to establish organization-defined "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) fraudulent actions.			Does the organization establish organization-defined "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) fraudulent actions?	7
Data Classification & Handling	Data Localization	DCH-26	Mechanisms exist to constrain the impact of "digital sovereignty laws," that require localized data within the host country, where data and processes may be subjected to arbitrary enforcement actions that potentially violate other applicable statutory, regulatory and/or contractual obligations.	- Board of Directors (Bod) Ethics Committee		Does the organization constrain the impact of "digital sovereignty laws," that require localized data within the host country, where data and processes may be subjected to arbitrary enforcement actions that potentially violate other applicable statutory, regulatory and/or contractual obligations?	10
Embedded Technology	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.		E-AST-07	Does the organization facilitate the implementation of embedded technology controls?	10
Embedded Technology	Internet of Things (IOT)	EMB-02	Mechanisms exist to proactively manage the cybersecurity and privacy risks associated with Internet of Things (IoT).			Does the organization proactively manage the cybersecurity and privacy risks associated with Internet of Things (IoT)?	9
Embedded Technology	Operational Technology (OT)	EMB-03	Mechanisms exist to proactively manage the cybersecurity and privacy risks associated with Operational Technology (OT).			Does the organization proactively manage the cybersecurity and privacy risks associated with Operational Technology (OT)?	9
Embedded Technology	Interface Security	EMB-04	Mechanisms exist to protect embedded devices against unauthorized use of the physical factory diagnostic and test interface(s).			Does the organization protect embedded devices against unauthorized use of the physical factory diagnostic and test interface(s)?	4
Embedded Technology	Embedded Technology Configuration Monitoring	EMB-05	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected.			Does the organization generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected?	6
Embedded Technology	Prevent Alterations	EMB-06	Mechanisms exist to protect embedded devices by preventing the unauthorized installation and execution of software.			Does the organization protect embedded devices by preventing the unauthorized installation and execution of software?	6
Embedded Technology	Embedded Technology Maintenance	EMB-07	Mechanisms exist to securely update software and upgrade functionality on embedded devices.			Does the organization securely updating software and upgrading functionality on embedded devices?	6
Embedded Technology	Resilience To Outages	EMB-08	Mechanisms exist to configure embedded technology to be resilient to data network and power outages.			Does the organization configure embedded technology to be resilient to outages of data networks and power?	2
Embedded Technology	Power Level Monitoring	EMB-09	Automated mechanisms exist to monitor the power levels of embedded technologies for decreased or excessive power usage, including battery drainage, to investigate for device tampering.			Does the organization continuously monitor the power levels of embedded technologies for decreased or excessive power usage, including battery drainage, to investigate for device tampering?	4
Embedded Technology	Embedded Technology Reviews	EMB-10	Mechanisms exist to perform evaluations of deployed embedded technologies as needed, or at least on an annual basis, to ensure that necessary updates to mitigate the risks associated with legacy embedded technologies are identified and implemented.			Does the organization perform evaluations of deployed embedded technologies as needed, or at least on an annual basis, to ensure that necessary updates to mitigate the risks associated with legacy embedded technologies are identified and implemented?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Embedded Technology	Message Queuing Telemetry Transport (MQTT) Security	EMB-11	Mechanisms exist to enforce the security of Message Queuing Telemetry Transport (MQTT) traffic.			Does the organization enforce the security of Message Queuing Telemetry Transport (MQTT) traffic?	7
Embedded Technology	Restrict Communications	EMB-12	Mechanisms exist to require embedded technologies to initiate all communications and drop new, incoming communications.			Does the organization require embedded technologies to initiate all communications and drop new, incoming communications?	8
Embedded Technology	Authorized Communications	EMB-13	Mechanisms exist to restrict embedded technologies to communicate only with authorized peers and service endpoints.			Does the organization restrict embedded technologies to communicate only with authorized peers and service endpoints?	8
Embedded Technology	Operating Environment Certification	EMB-14	Mechanisms exist to determine if embedded technologies are certified for secure use in the proposed operating environment.			Does the organization determine if embedded technologies are certified for use in the proposed operating environment?	9
Embedded Technology	Safety Assessment	EMB-15	Mechanisms exist to evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure.			Does the organization evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure?	9
Embedded Technology	Certificate-Based Authentication	EMB-16	Mechanisms exist to enforce certificate-based authentication for embedded technologies (e.g., IoT, OT, etc.) and their supporting services.			Does the organization enforce certificate-based authentication for embedded technologies (e.g., IoT, OT, etc.) and their supporting services?	5
Embedded Technology	Chip-To-Cloud Security	EMB-17	Mechanisms exist to implement embedded technologies that utilize pre-provisioned cloud trust anchors to support secure bootstrap and Zero Touch Provisioning (ZTP).			Does the organization implement embedded technologies that utilize pre-provisioned cloud trust anchors to support secure bootstrap and Zero Touch Provisioning (ZTP)?	6
Embedded Technology	Real-Time Operating System (RTOS) Security	EMB-18	Mechanisms exist to ensure embedded technologies utilize a securely configured Real-Time Operating System (RTOS).			Does the organization ensure embedded technologies utilize a securely configured Real-Time Operating System (RTOS)?	5
Embedded Technology	Safe Operations	EMB-19	Mechanisms exist to continuously validate autonomous systems that trigger an automatic state change when safe operation is no longer assured.			Does the organization continuously validate autonomous systems that trigger an automatic state change when safe operation is no longer assured?	9
Endpoint Security	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Group Policy Objects (GPOs) - Antimalware technologies - Software firewalls		Does the organization facilitate the implementation of endpoint security controls?	10
Endpoint Security	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization protect the confidentiality, integrity, availability and safety of endpoint devices?	9
Endpoint Security	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Removal of local admin rights - Privileged Account Management (PAM) - NNT Change Tracker		Does the organization prohibit user installation of software without explicitly assigned privileged status?	9
Endpoint Security	Software Installation Alerts	END-03.1	Mechanisms exist to generate an alert when new software is detected.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization alert personnel when an unauthorized installation of software is detected?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Endpoint Security	Governing Access Restriction for Change	END-03.2	Mechanisms exist to define, document, approve and enforce access restrictions associated with changes to systems.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization define, document, approve and enforce access restrictions associated with changes to systems?	8
Endpoint Security	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - Antimalware software - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization utilize antimalware technologies to detect and eradicate malicious code?	10
Endpoint Security	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	- Antimalware software		Does the organization automatically update antimalware technologies, including signature definitions?	9
Endpoint Security	Documented Protection Measures	END-04.2	Mechanisms exist to document antimalware technologies.			Does the organization document antimalware technologies?	3
Endpoint Security	Centralized Management of Antimalware Technologies	END-04.3	Mechanisms exist to centrally-manage antimalware technologies.	- Antimalware software	E-MON-02	Does the organization centrally-manage antimalware technologies?	8
Endpoint Security	Heuristic / Nonsignature-Based Detection	END-04.4	Mechanisms exist to utilize heuristic / nonsignature-based antimalware detection capabilities.	- Antimalware software		Does the organization utilize heuristic / nonsignature-based antimalware detection capabilities?	8
Endpoint Security	Malware Protection Mechanism Testing	END-04.5	Mechanisms exist to test antimalware technologies by introducing a known benign, non-spreading test case into the system and subsequently verifying that both detection of the test case and associated incident reporting occurs.	- EICAR test file		Does the organization test antimalware technologies by introducing a known benign, non-spreading test case into the system and subsequently verifying that both detection of the test case and associated incident reporting occurs?	5
Endpoint Security	Evolving Malware Threats	END-04.6	Mechanisms exist to perform periodic evaluations evolving malware threats to assess systems that are generally not considered to be commonly affected by malicious software.			Does the organization perform periodic evaluations evolving malware threats to assess systems that are generally not considered to be commonly affected by malicious software?	3
Endpoint Security	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	- Antimalware software		Does the organization ensure that anti-malware technologies are continuously running and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period?	9
Endpoint Security	Software Firewall	END-05	Mechanisms exist to utilize host-based firewall software, or a similar technology, on all information systems, where technically feasible.	- NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization utilize host-based firewall software, or a similar technology, on all information systems, where technically feasible?	9
Endpoint Security	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM) technology to detect and report unauthorized changes to system files and configurations.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com) - File Integrity Monitor (FIM)		Does the organization utilize File Integrity Monitor (FIM) technology to detect and report unauthorized changes to system files and configurations?	8
Endpoint Security	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com) - File Integrity Monitor (FIM)		Does the organization validate configurations through integrity checking of software and firmware?	6
Endpoint Security	Integration of Detection & Response	END-06.2	Mechanisms exist to detect and respond to unauthorized configuration changes as cybersecurity incidents.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com) - File Integrity Monitor (FIM)		Does the organization detect and respond to unauthorized configuration changes as cybersecurity incidents?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Endpoint Security	Automated Notifications of Integrity Violations	END-06.3	Automated mechanisms exist to alert incident response personnel upon discovering discrepancies during integrity verification.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization alert incident response personnel upon discovering discrepancies during integrity verification?	5
Endpoint Security	Automated Response to Integrity Violations	END-06.4	Automated mechanisms exist to implement remediation actions when integrity violations are discovered.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization implement remediation actions when integrity violations are discovered?	5
Endpoint Security	Boot Process Integrity	END-06.5	Automated mechanisms exist to verify the integrity of the boot process of information systems.			Does the organization use automated mechanisms to verify the integrity of the boot process of information systems?	5
Endpoint Security	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in information systems.			Does the organization protect the integrity of boot firmware in information systems?	5
Endpoint Security	Binary or Machine-Executable Code	END-06.7	Mechanisms exist to prohibit the use of binary or machine-executable code from sources with limited or no warranty and without access to source code.			Does the organization prohibit the use of binary or machine-executable code from sources with limited or no warranty and without access to source code?	5
Endpoint Security	Host Intrusion Detection and Prevention Systems (HIDS / HIPS)	END-07	Mechanisms exist to utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS) on sensitive systems.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com) - File Integrity Monitor (FIM)		Does the organization utilize Host-based Intrusion Detection / Prevention Systems (HIDS / HIPS) on sensitive systems?	9
Endpoint Security	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.			Does the organization utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail?	10
Endpoint Security	Central Management	END-08.1	Mechanisms exist to centrally-manage anti-phishing and spam protection technologies.			Does the organization centrally-manage anti-phishing and spam protection technologies?	5
Endpoint Security	Automatic Spam and Phishing Protection Updates	END-08.2	Mechanisms exist to automatically update anti-phishing and spam protection technologies when new releases are available in accordance with configuration and change management practices.			Does the organization automatically update anti-phishing and spam protection technologies when new releases are available in accordance with configuration and change management practices?	8
Endpoint Security	Trusted Path	END-09	Mechanisms exist to establish a trusted communications path between the user and the security functions of the operating system.	- Active Directory (AD) Ctrl+Alt+Del login process		Does the organization establish a trusted communications path between the user and the security functions of the operating system?	9
Endpoint Security	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.			Does the organization address mobile code / operating system-independent applications?	4
Endpoint Security	Thin Nodes	END-11	Mechanisms exist to configure thin nodes to have minimal functionality and information storage.			Does the organization configure thin nodes to have minimal functionality and information storage?	4
Endpoint Security	Port & Input / Output (I/O) Device Access	END-12	Mechanisms exist to physically disable or remove unnecessary connection ports or input/output devices from sensitive systems.			Does the organization physically disable or remove unnecessary connection ports or input/output devices from sensitive systems?	6

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Endpoint Security	Sensor Capability	END-13	Mechanisms exist to configure embedded sensors on systems to: • Prohibit the remote activation of sensing capabilities; and • Provide an explicit indication of sensor use to users.			Does the organization configure embedded sensors on systems to: • Prohibit the remote activation of sensing capabilities; and • Provide an explicit indication of sensor use to users?	7
Endpoint Security	Authorized Use	END-13.1	Mechanisms exist to utilize organization-defined measures so that data or information collected by sensors is only used for authorized purposes.			Does the organization utilize organization-defined measures so that data or information collected by sensors is only used for authorized purposes?	8
Endpoint Security	Notice of Collection	END-13.2	Mechanisms exist to notify individuals that Personal Data (PD) is collected by sensors.	- Visible or auditory alert - Data Protection Impact Assessment (DPIA)		Does the organization notify individuals that Personal Data (PD) is collected by sensors?	6
Endpoint Security	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.			Does the organization utilize sensors that are configured to minimize the collection of information about individuals?	8
Embedded Technology	Sensor Delivery Verification	END-13.4	Mechanisms exist to verify embedded technology sensors are configured so that data collected by the sensor(s) is only reported to authorized individuals or roles.			Does the organization verify embedded technology sensors are configured so that data collected by the sensor(s) is only reported to authorized individuals or roles?	4
Endpoint Security	Collaborative Computing Devices	END-14	Mechanisms exist to unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: • Networked whiteboards; • Video teleconference cameras; and • Teleconference microphones.	- Unplug devices when not needed		Does the organization unplug or prohibit the remote activation of collaborative computing devices with the following exceptions: • Networked whiteboards; • Video teleconference cameras; and • Teleconference microphones?	9
Endpoint Security	Disabling / Removal In Secure Work Areas	END-14.1	Mechanisms exist to disable or remove collaborative computing devices from critical information systems and secure work areas.			Does the organization disable or remove collaborative computing devices from critical information systems and secure work areas?	5
Endpoint Security	Explicitly Indicate Current Participants	END-14.2	Automated mechanisms exist to provide an explicit indication of current participants in online meetings and teleconferences.			Does the organization provide an explicit indication of current participants in online meetings and teleconferences?	5
Endpoint Security	Hypervisor Access	END-15	Mechanisms exist to restrict access to hypervisor management functions or administrative consoles for systems hosting virtualized systems.			Does the organization restrict access to hypervisor management functions or administrative consoles for systems hosting virtualized systems?	9
Endpoint Security	Restrict Access To Security Functions	END-16	Mechanisms exist to ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions.	- Windows Defender Device Guard		Does the organization ensure security functions are restricted to authorized individuals and enforce least privilege control requirements for necessary job functions?	7
Endpoint Security	Host-Based Security Function Isolation	END-16.1	Mechanisms exist to implement underlying software separation mechanisms to facilitate security function isolation.	- Windows Defender Device Guard		Does the organization implement underlying software separation mechanisms to facilitate security function isolation?	7
Human Resources Security	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.			Does the organization facilitate the implementation of personnel security controls?	10
Human Resources Security	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.		E-HRS-01 E-HRS-02 E-HRS-03 E-HRS-04 E-HRS-11 E-HRS-22	Does the organization manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Human Resources Security	Users With Elevated Privileges	HRS-02.1	Mechanisms exist to ensure that every user accessing a system that processes, stores, or transmits sensitive information is cleared and regularly trained to handle the information in question.		E-HRS-02 E-HRS-03 E-HRS-04 E-HRS-11 E-HRS-22	Does the organization ensure that every user accessing a system that processes, stores, or transmits sensitive information is cleared and regularly trained to handle the information in question?	10
Human Resources Security	Probationary Periods	HRS-02.2	Mechanisms exist to identify newly onboarded personnel for enhanced monitoring during their probationary period.			Does the organization identify newly onboarded personnel through their probationary period to implement enhanced monitoring?	1
Human Resources Security	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	- NIST NICE framework - RACI diagram	E-HRS-01 E-HRS-02 E-HRS-03 E-HRS-04 E-HRS-11 E-HRS-13	Does the organization define cybersecurity responsibilities for all personnel?	10
Human Resources Security	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.		E-HRS-01 E-HRS-13 E-HRS-16 E-HRS-18	Does the organization communicate with users about their roles and responsibilities to maintain a safe and secure working environment?	9
Human Resources Security	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.		E-HRS-21 E-HRS-23	Does the organization ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set?	9
Human Resources Security	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	- Criminal, education and employment background checks	E-HRS-17 E-HRS-21	Does the organization manage personnel security risk by screening individuals prior to authorizing access?	10
Human Resources Security	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	- Security clearances for classified information.	E-HRS-17 E-HRS-21	Does the organization ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria?	9
Human Resources Security	Formal Indoctrination	HRS-04.2	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information are formally indoctrinated for all the relevant types of information to which they have access on the system.		E-HRS-18	Does the organization verify that individuals accessing a system processing, storing, or transmitting sensitive information are formally indoctrinated for all the relevant types of information to which they have access on the system?	7
Human Resources Security	Citizenship Requirements	HRS-04.3	Mechanisms exist to verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship.			Does the organization verify that individuals accessing a system processing, storing, or transmitting sensitive information meet applicable statutory, regulatory and/or contractual requirements for citizenship?	5
Human Resources Security	Citizenship Identification	HRS-04.4	Mechanisms exist to identify foreign nationals, including by their specific citizenship.			Does the organization identify foreign nationals, including by their specific nationality?	3
Human Resources Security	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and privacy principles in their daily work.	- Acceptable Use Policy (AUP) - Rules of behavior	E-HRS-16 E-HRS-22	Does the organization require all employees and contractors to apply cybersecurity and privacy principles in their daily work?	10
Human Resources Security	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	- Acceptable Use Policy (AUP) - Rules of behavior	E-HRS-22	Does the organization define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior?	10
Human Resources Security	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	- Acceptable Use Policy (AUP) - Rules of behavior	E-HRS-22	Do rules of behavior contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Human Resources Security	Use of Communications Technology	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously.	- Acceptable Use Policy (AUP) - Rules of behavior	E-HRS-22	Does the organization establish usage restrictions and implementation guidance for communications technologies based on the potential to cause damage to systems, if used maliciously?	10
Human Resources Security	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.		E-HRS-22	Does the organization govern usage policies for critical technologies?	9
Human Resources Security	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	- Acceptable Use Policy (AUP) - Rules of behavior - BYOD policy	E-HRS-22	Does the organization manage business risks associated with permitting mobile device access to organizational resources?	9
Human Resources Security	Security-Minded Dress Code	HRS-05.6	Mechanisms exist to prohibit the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts, etc.) to prevent the unauthorized exfiltration of data and technology assets.			Does the organization prohibit the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts, etc.) to prevent the unauthorized exfiltration of data and technology assets?	1
Human Resources Security	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity and privacy policies and provide acknowledgement.		E-HRS-18 E-SAT-02 E-SAT-04	Does the organization ensure personnel receive recurring familiarization with the organization's cybersecurity and privacy policies and provide acknowledgement?	8
Human Resources Security	Access Agreements	HRS-06	Mechanisms exist to require internal and third-party users to sign appropriate access agreements prior to being granted access.		E-HRS-16	Does the organization require internal and third-party users to sign appropriate access agreements prior to being granted access?	10
Human Resources Security	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	- Non-Disclosure Agreements (NDAs)	E-HRS-20	Does the organization require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties?	10
Human Resources Security	Post-Employment Obligations	HRS-06.2	Mechanisms exist to notify terminated individuals of applicable, legally-binding post-employment requirements for the protection of sensitive organizational information.		E-HRS-19	Does the organization notify terminated individuals of applicable, legally-binding post-employment requirements for the protection of sensitive organizational information?	5
Human Resources Security	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.			Does the organization sanction personnel failing to comply with established security policies, standards and procedures?	9
Human Resources Security	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.			Does the organization conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated?	8
Human Resources Security	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.			Does the organization adjust logical and physical access authorizations to systems and facilities upon personnel reassignment or transfer, in a timely manner?	9
Human Resources Security	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.		E-HRS-19	Does the organization govern the termination of individual employment?	9
Human Resources Security	Asset Collection	HRS-09.1	Mechanisms exist to retrieve organization-owned assets upon termination of an individual's employment.		E-HRS-19	Does the organization retrieve organization-owned assets upon termination of an individual's employment?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Human Resources Security	High-Risk Terminations	HRS-09.2	Mechanisms exist to expedite the process of removing "high risk" individual's access to systems and applications upon termination, as determined by management.		E-HRS-19	Does the organization expedite the process of removing "high risk" individual's access to systems and applications upon termination, as determined by management?	9
Human Resources Security	Post-Employment Requirements	HRS-09.3	Mechanisms exist to govern former employee behavior by notifying terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information.	- Non-Disclosure Agreements (NDAs)	E-HRS-19	Does the organization govern former employee behavior by notifying terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information?	8
Human Resources Security	Automated Employment Status Notifications	HRS-09.4	Automated mechanisms exist to notify Identity and Access Management (IAM) personnel or roles upon termination of an individual employment or contract.			Does the organization notify Identity and Access Management (IAM) personnel or roles upon termination of an individual employment or contract?	5
Human Resources Security	Third-Party Personnel Security	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party cybersecurity and privacy roles and responsibilities.	- Independent background check service	E-HRS-16 E-HRS-18 E-HRS-22	Does the organization govern third-party personnel by reviewing and monitoring third-party cybersecurity and privacy roles and responsibilities?	10
Human Resources Security	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.		E-HRS-25	Does the organization implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion?	7
Human Resources Security	Incompatible Roles	HRS-12	Mechanisms exist to avoid incompatible development-specific roles through limiting and reviewing developer privileges to change hardware, software and firmware components within a production/operational environment.		E-HRS-25	Does the organization avoid incompatible development-specific roles through limiting and reviewing developer privileges to change hardware, software and firmware components within a production/operational environment?	8
Human Resources Security	Two-Person Rule	HRS-12.1	Mechanisms exist to enforce a two-person rule for implementing changes to sensitive systems.			Does the organization enforce a two-person rule for implementing changes to sensitive systems?	7
Human Resources Security	Identify Critical Skills & Gaps	HRS-13	Mechanisms exist to evaluate the critical cybersecurity and privacy skills needed to support the organization's mission and identify gaps that exist.		E-HRS-23 E-HRS-24	Does the organization evaluate the critical cybersecurity and privacy skills needed to support the organization's mission and identify gaps that exist?	5
Human Resources Security	Remediate Identified Skills Deficiencies	HRS-13.1	Mechanisms exist to remediate critical skills deficiencies necessary to support the organization's mission and business functions.		E-HRS-24	Does the organization remediate critical skills deficiencies necessary to support the organization's mission and business functions?	5
Human Resources Security	Identify Vital Cybersecurity & Privacy Staff	HRS-13.2	Mechanisms exist to identify vital cybersecurity & privacy staff.		E-HRS-26	Does the organization identify vital cybersecurity & privacy staff?	5
Human Resources Security	Establish Redundancy for Vital Cybersecurity & Privacy Staff	HRS-13.3	Mechanisms exist to establish redundancy for vital cybersecurity & privacy staff.			Does the organization establish redundancy for vital cybersecurity & privacy staff?	5
Human Resources Security	Perform Succession Planning	HRS-13.4	Mechanisms exist to perform succession planning for vital cybersecurity & privacy roles.			Does the organization perform succession planning for vital cybersecurity & privacy roles?	5
Identification & Authentication	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.			Does the organization facilitate the implementation of identification and access management controls?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Identification & Authentication	Retain Access Records	IAC-01.1	Mechanisms exist to retain a record of personnel accountability to ensure there is a record of all access granted to an individual (system and application-wise), who provided the authorization, when the authorization was granted and when the access was last reviewed.			Does the organization retain a record of personnel accountability to ensure there is a record of all personnel authorized to access a system, their user identification, who provided the authorization, when the authorization was granted and when the access was last reviewed?	3
Identification & Authentication	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.			Does the organization uniquely identify and authenticate organizational users and processes acting on behalf of organizational users?	9
Identification & Authentication	Group Authentication	IAC-02.1	Mechanisms exist to require individuals to be authenticated with an individual authenticator when a group authenticator is utilized.			Does the organization require individuals to be authenticated with an individual authenticator when a group authenticator is utilized?	7
Identification & Authentication	Network Access to Privileged Accounts - Replay Resistant	IAC-02.2	Automated mechanisms exist to employ replay-resistant network access authentication.			Does the organization employ replay-resistant network access authentication?	9
Identification & Authentication	Acceptance of PIV Credentials	IAC-02.3	Mechanisms exist to accept and electronically verify organizational Personal Identity Verification (PIV) credentials.	- Personal Identity Verification (PIV) credentials		Does the organization accept and electronically verify organizational Personal Identity Verification (PIV) credentials?	2
Identification & Authentication	Out-of-Band Authentication (OOBA)	IAC-02.4	Mechanisms exist to implement Out-of-Band Authentication (OOBA) under specific conditions.			Does the organization implement Out-of-Band Authentication (OOBA) under specific conditions?	5
Identification & Authentication	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.			Does the organization uniquely and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization?	9
Identification & Authentication	Acceptance of PIV Credentials from Other Organizations	IAC-03.1	Mechanisms exist to accept and electronically verify Personal Identity Verification (PIV) credentials from third-parties.			Does the organization accept and electronically verify Personal Identity Verification (PIV) credentials from third-parties?	2
Identification & Authentication	Acceptance of Third-Party Credentials	IAC-03.2	Automated mechanisms exist to accept Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials.			Does the organization accept Federal Identity, Credential and Access Management (FICAM)-approved third-party credentials?	2
Identification & Authentication	Use of FICAM-Issued Profiles	IAC-03.3	Mechanisms exist to conform systems to Federal Identity, Credential and Access Management (FICAM)-issued profiles.			Does the organization conform systems to Federal Identity, Credential and Access Management (FICAM)-issued profiles?	2
Identification & Authentication	Disassociability	IAC-03.4	Mechanisms exist to disassociate user attributes or credential assertion relationships among individuals, credential service providers and relying parties.			Does the organization disassociate user attributes or credential assertion relationships among individuals, credential service providers and relying parties?	2
Identification & Authentication	Acceptance of External Authenticators	IAC-03.5	Mechanisms exist to restrict the use of external authenticators to those that are National Institute of Standards and Technology (NIST)-compliant and maintain a list of accepted external authenticators.			Does the organization restrict the use of external authenticators to those that are National Institute of Standards and Technology (NIST)-compliant and maintain a list of accepted external authenticators?	4
Identification & Authentication	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	- Active Directory (AD) Kerberos		Does the organization uniquely and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Identification & Authentication	Device Attestation	IAC-04.1	Mechanisms exist to ensure device identification and authentication is accurate by centrally-managing the joining of systems to the domain as part of the initial asset configuration management process.			Does the organization ensure device identification and authentication is accurate by centrally-managing the joining of systems to the domain as part of the initial asset configuration management process?	5
Identification & Authentication	Identification & Authentication for Third Party Systems & Services	IAC-05	Mechanisms exist to identify and authenticate third-party systems and services.			Does the organization identify and authenticate third-party systems and services?	9
Identification & Authentication	Sharing Identification & Authentication Information	IAC-05.1	Mechanisms exist to ensure third-party service providers provide current and accurate information for any third-party user with access to the organization's data or assets.			Does the organization ensure third-party service providers provide current and accurate information for any third-party user with access to the organization's data or assets?	5
Identification & Authentication	Privileged Access by Non-Organizational Users	IAC-05.2	Mechanisms exist to prohibit privileged access by non-organizational users.			Does the organization prohibit privileged access by non-organizational users?	9
Identification & Authentication	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: • Remote network access; • Third-party systems, applications and/or services; and/ or • Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	- Multi-Factor Authentication (MFA) - Microsoft Active Directory (AD) Certificate Services - Yubico (https://www.yubico.com) - Duo (https://www.duo.com)		Does the organization require Multi-Factor Authentication (MFA) for remote network access?	9
Identification & Authentication	Network Access to Privileged Accounts	IAC-06.1	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	- Multi-Factor Authentication (MFA) - Microsoft Active Directory (AD) Certificate Services - Yubico (https://www.yubico.com) - Duo (https://www.duo.com)		Does the organization utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts?	9
Identification & Authentication	Network Access to Non-Privileged Accounts	IAC-06.2	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts.	- Multi-Factor Authentication (MFA) - Microsoft Active Directory (AD) Certificate Services - Yubico (https://www.yubico.com) - Duo (https://www.duo.com)		Does the organization utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts?	7
Identification & Authentication	Local Access to Privileged Accounts	IAC-06.3	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	- Multi-Factor Authentication (MFA) - Microsoft Active Directory (AD) Certificate Services - Yubico (https://www.yubico.com) - Duo (https://www.duo.com)		Does the organization utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts?	5
Identification & Authentication	Out-of-Band Multi-Factor Authentication	IAC-06.4	Mechanisms exist to implement Multi-Factor Authentication (MFA) for remote access to privileged and non-privileged accounts such that one of the factors is securely provided by a device separate from the system gaining access.			Does the organization implement Multi-Factor Authentication (MFA) for remote access to privileged and non-privileged accounts such that one of the factors is securely provided by a device separate from the system gaining access?	5
Identification & Authentication	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.		E-HRS-12 E-HRS-18 E-HRS-19	Does the organization utilize a formal user registration and de-registration process that governs the assignment of access rights?	10
Identification & Authentication	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.		E-HRS-12 E-HRS-19	Does the organization revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted?	10
Identification & Authentication	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.		E-HRS-19	Does the organization revoke user access rights in a timely manner, upon termination of employment or contract?	10
Identification & Authentication	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.	- Role-Based Access Control (RBAC)	E-HRS-12 E-IAM-02	Does the organization enforce a Role-Based Access Control (RBAC) policy over users and resources?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Identification & Authentication	Identifier Management (User Names)	IAC-09	Mechanisms exist to govern naming standards for usernames and systems.			Does the organization govern naming standards for usernames and systems?	9
Identification & Authentication	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.			Does the organization ensure proper user identification management for non-consumer users and administrators?	9
Identification & Authentication	Identity User Status	IAC-09.2	Mechanisms exist to identify contractors and other third-party users through unique username characteristics.			Does the organization identify contractors and other third-party users through unique username characteristics?	7
Identification & Authentication	Dynamic Management	IAC-09.3	Mechanisms exist to dynamically manage usernames and system identifiers.	- Microsoft Active Directory (AD)		Does the organization dynamically manage usernames and system identifiers?	5
Identification & Authentication	Cross-Organization Management	IAC-09.4	Mechanisms exist to coordinate username identifiers with external organizations for cross-organization management of identifiers.			Does the organization coordinate username identifiers with external organizations for cross-organization management of identifiers?	5
Identification & Authentication	Privileged Account Identifiers	IAC-09.5	Mechanisms exist to uniquely manage privileged accounts to identify the account as a privileged user or service.			Does the organization uniquely manage privileged accounts to identify the account as a privileged user or service?	9
Identification & Authentication	Pairwise Pseudonymous Identifiers (PPID)	IAC-09.6	Mechanisms exist to generate pairwise pseudonymous identifiers with no identifying information about a data subject to discourage activity tracking and profiling of the data subject.			Does the organization generate pairwise pseudonymous identifiers with no identifying information about a subscriber to discourage activity tracking and profiling of the subscriber?	1
Identification & Authentication	Authenticator Management	IAC-10	Mechanisms exist to securely manage authenticators for users and devices.			Does the organization securely manage authenticators for users and devices?	10
Identification & Authentication	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.			Does the organization enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication?	9
Identification & Authentication	PKI-Based Authentication	IAC-10.2	Automated mechanisms exist to validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication.			Does the organization validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information for PKI-based authentication?	9
Identification & Authentication	In-Person or Trusted Third-Party Registration	IAC-10.3	Mechanisms exist to conduct in-person or trusted third-party identify verification before user accounts for third-parties are created.			Does the organization conduct in-person or trusted third-party identify verification before user accounts for third-parties are created?	9
Identification & Authentication	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.			Does the organization use automated mechanisms to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements?	5
Identification & Authentication	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.			Does the organization protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Identification & Authentication	No Embedded Unencrypted Static Authenticators	IAC-10.6	Mechanisms exist to ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys.			Does the organization ensure that unencrypted, static authenticators are not embedded in applications, scripts or stored on function keys?	10
Identification & Authentication	Hardware Token-Based Authentication	IAC-10.7	Automated mechanisms exist to ensure organization-defined token quality requirements are satisfied for hardware token-based authentication.	- Tokens are sufficiently encrypted or do not reveal credentials or passwords within the token.		Does the organization ensure organization-defined token quality requirements are satisfied for hardware token-based authentication?	9
Identification & Authentication	Vendor-Supplied Defaults	IAC-10.8	Mechanisms exist to ensure vendor-supplied defaults are changed as part of the installation process.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization ensure vendor-supplied defaults are changed as part of the installation process?	10
Identification & Authentication	Multiple Information System Accounts	IAC-10.9	Mechanisms exist to implement security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems.			Does the organization implement security safeguards to manage the risk of compromise due to individuals having accounts on multiple information systems?	5
Identification & Authentication	Expiration of Cached Authenticators	IAC-10.10	Automated mechanisms exist to prohibit the use of cached authenticators after organization-defined time period.			Does the organization prohibit the use of cached authenticators after organization-defined time period?	5
Identification & Authentication	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.			Does the organization protect and store passwords via a password manager tool?	8
Identification & Authentication	Biometric Authentication	IAC-10.12	Mechanisms exist to ensure biometric-based authentication satisfies organization-defined biometric quality requirements for false positives and false negatives.			Does the organization ensure biometric-based authentication satisfies organization-defined biometric quality requirements for false positives and false negatives?	5
Identification & Authentication	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.			Does the organization obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals?	6
Identification & Authentication	Cryptographic Module Authentication	IAC-12	Mechanisms exist to ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength.	- FIPS 140-2		Does the organization ensure cryptographic modules adhere to applicable statutory, regulatory and contractual requirements for security strength?	8
Identification & Authentication	Hardware Security Modules (HSM)	IAC-12.1	Automated mechanisms exist to utilize Hardware Security Modules (HSM) to protect authenticators on which the component relies.			Does the organization utilize Hardware Security Modules (HSM) to protect authenticators?	3
Identification & Authentication	Adaptive Identification & Authentication	IAC-13	Mechanisms exist to allow individuals to utilize alternative methods of authentication under specific circumstances or situations.			Does the organization allow individuals to utilize alternative methods of authentication under specific circumstances or situations?	5
Identification & Authentication	Single Sign-On (SSO)	IAC-13.1	Mechanisms exist to provide a Single Sign-On (SSO) capability to the organization's systems and services.			Does the organization provide a Single Sign-On (SSO) capability to the organization's systems and services?	5
Identification & Authentication	Federated Credential Management	IAC-13.2	Mechanisms exist to federate credentials to allow cross-organization authentication of individuals and devices.			Does the organization federate credentials to allow cross-organization authentication of individuals and devices?	4

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Identification & Authentication	Re-Authentication	IAC-14	Mechanisms exist to force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication.			Does the organization force users and devices to re-authenticate according to organization-defined circumstances that necessitate re-authentication?	8
Identification & Authentication	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	- Service accounts prohibit interactive login - users cannot log into systems with those accounts.		Does the organization proactively govern account management of individual, group, system, application, guest and temporary accounts?	10
Identification & Authentication	Automated System Account Management	IAC-15.1	Automated mechanisms exist to support the management of system accounts.	- Service accounts prohibit interactive login - users cannot log into systems with those accounts.		Does the organization use automated mechanisms to support the management of system accounts?	5
Identification & Authentication	Removal of Temporary / Emergency Accounts	IAC-15.2	Automated mechanisms exist to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account.			Does the organization use automated mechanisms to disable or remove temporary and emergency accounts after an organization-defined time period for each type of account?	9
Identification & Authentication	Disable Inactive Accounts	IAC-15.3	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.			Does the organization use automated mechanisms to disable inactive accounts after an organization-defined time period?	10
Identification & Authentication	Automated Audit Actions	IAC-15.4	Automated mechanisms exist to audit account creation, modification, enabling, disabling and removal actions and notify organization-defined personnel or roles.			Does the organization use automated mechanisms to audit account creation, modification, enabling, disabling and removal actions and notify organization-defined personnel or roles?	5
Identification & Authentication	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.			Does the organization authorize the use of shared/group accounts only under certain organization-defined conditions?	10
Identification & Authentication	Account Disabling for High Risk Individuals	IAC-15.6	Mechanisms exist to disable accounts immediately upon notification for users posing a significant risk to the organization.			Does the organization disable accounts immediately upon notification for users posing a significant risk to the organization?	10
Identification & Authentication	System Accounts	IAC-15.7	Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner.			Does the organization review all system accounts and disable any account that cannot be associated with a business process and owner?	10
Identification & Authentication	Usage Conditions	IAC-15.8	Automated mechanisms exist to enforce usage conditions for users and/or roles.			Does the organization enforce usage conditions for users and/or roles?	5
Identification & Authentication	Emergency Accounts	IAC-15.9	Mechanisms exist to establish and control "emergency access only" accounts.			Does the organization establish and control "emergency access only" accounts?	5
Identification & Authentication	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.		E-IAM-03	Does the organization restrict and control privileged access rights for users and services?	10
Identification & Authentication	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.		E-IAM-03	Does the organization inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Identification & Authentication	Privileged Account Separation	IAC-16.2	Mechanisms exist to separate privileged accounts between infrastructure environments to reduce the risk of a compromise in one infrastructure environment from laterally affecting other infrastructure environments.			Does the organization separate privileged accounts between infrastructure environments to reduce the risk of a compromise in one infrastructure environment from laterally affecting other infrastructure environments?	4
Identification & Authentication	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.		E-HRS-12 E-HRS-14 E-IAM-01	Does the organization periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary?	10
Identification & Authentication	User Responsibilities for Account Management	IAC-18	Mechanisms exist to compel users to follow accepted practices in the use of authentication mechanisms (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.).	- Employment contract - Rules of Behavior - Formalized password policy		Does the organization compel users to follow accepted practices in the use of authentication mechanisms (e.g. passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.)?	10
Identification & Authentication	Credential Sharing	IAC-19	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.			Does the organization prevent the sharing of generic IDs, passwords or other generic authentication methods?	10
Identification & Authentication	Access Enforcement	IAC-20	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."			Does the organization enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege?"	10
Identification & Authentication	Access To Sensitive Data	IAC-20.1	Mechanisms exist to limit access to sensitive/regulated data to only those individuals whose job requires such access.			Does the organization limit access to sensitive/regulated data to only those individuals whose job requires such access?	10
Identification & Authentication	Database Access	IAC-20.2	Mechanisms exist to restrict access to databases containing sensitive/regulated data to only necessary services or those individuals whose job requires such access.			Does the organization restrict access to databases containing sensitive/regulated data to only necessary services or those individuals whose job requires such access?	10
Identification & Authentication	Use of Privileged Utility Programs	IAC-20.3	Mechanisms exist to restrict and tightly control utility programs that are capable of overriding system and application controls.			Does the organization restrict and tightly control utility programs that are capable of overriding system and application controls?	9
Identification & Authentication	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	- Jump hosts		Does the organization restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine?	8
Identification & Authentication	Dual Authorization for Privileged Commands	IAC-20.5	Automated mechanisms exist to enforce dual authorization for privileged commands.			Does the organization enforce dual authorization for privileged commands?	5
Identification & Authentication	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.			Does the organization revoke logical and physical access authorizations?	9
Identification & Authentication	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.			Does the organization utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions?	10
Identification & Authentication	Authorize Access to Security Functions	IAC-21.1	Mechanisms exist to limit access to security functions to explicitly-authorized privileged users.			Does the organization limit access to security functions to explicitly-authorized privileged users?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Identification & Authentication	Non-Privileged Access for Non-Security Functions	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.			Does the organization prohibit privileged users from using privileged accounts, while performing non-security functions?	9
Identification & Authentication	Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to organization-defined personnel or roles without management approval.			Does the organization restrict the assignment of privileged accounts to organization-defined personnel or roles without management approval?	10
Identification & Authentication	Auditing Use of Privileged Functions	IAC-21.4	Mechanisms exist to audit the execution of privileged functions.			Does the organization audit the execution of privileged functions?	9
Identification & Authentication	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.			Does the organization prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures?	9
Identification & Authentication	Network Access to Privileged Commands	IAC-21.6	Mechanisms exist to authorize remote access to perform privileged commands on critical systems or where sensitive/regulated data is stored, transmitted and/or processed only for compelling operational needs.			Does the organization authorize remote access to perform privileged commands on critical systems or where sensitive/regulated data is stored, transmitted and/or processed only for compelling operational needs?	5
Identification & Authentication	Privilege Levels for Code Execution	IAC-21.7	Automated mechanisms exist to prevent applications from executing at higher privilege levels than the user's privileges.			Does the organization prevent applications from executing at higher privilege levels than the user's privileges?	5
Identification & Authentication	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.			Does the organization enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded?	9
Identification & Authentication	Concurrent Session Control	IAC-23	Mechanisms exist to limit the number of concurrent sessions for each system account.			Does the organization limit the number of concurrent sessions for each system account?	6
Identification & Authentication	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.			Does the organization initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods?	9
Identification & Authentication	Pattern-Hiding Displays	IAC-24.1	Mechanisms exist to implement pattern-hiding displays to conceal information previously visible on the display during the session lock.			Does the organization implement pattern-hiding displays to conceal information previously visible on the display during the session lock?	9
Identification & Authentication	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.			Does the organization use automated mechanisms to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity?	9
Identification & Authentication	User-Initiated Logouts / Message Displays	IAC-25.1	Mechanisms exist to provide a logout capability and display an explicit logout message to users indicating the reliable termination of the session.			Does the organization provide a logout capability and display an explicit logout message to users indicating the reliable termination of the session?	5
Identification & Authentication	Permitted Actions Without Identification or Authorization	IAC-26	Mechanisms exist to identify and document the supporting rationale for specific user actions that can be performed on a system without identification or authentication.			Does the organization identify and document the supporting rationale for specific user actions that can be performed on a system without identification or authentication?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Identification & Authentication	Reference Monitor	IAC-27	Mechanisms exist to implement a reference monitor that is tamperproof, always-invoked, small enough to be subject to analysis / testing and the completeness of which can be assured.			Does the organization implement a reference monitor that is tamperproof, always-invoked, small enough to be subject to analysis / testing and the completeness of which can be assured?	1
Identification & Authentication	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before modifying any permissions or authentication factor.	- Professional references - Education / certification transcripts - Driver's license - Passport		Does the organization collect, validate and verify identity evidence of a user?	10
Identification & Authentication	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.			Does the organization require the registration process to receive management approval for new accounts or changes in permissions to existing accounts?	10
Identification & Authentication	Identity Evidence	IAC-28.2	Mechanisms exist to require evidence of individual identification to be presented to the registration authority.	- Driver's license - Passport		Does the organization require evidence of individual identification to be presented to the registration authority?	5
Identification & Authentication	Identity Evidence Validation & Verification	IAC-28.3	Mechanisms exist to require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification.	- Employment verification - Credit check - Criminal history check - Education verification		Does the organization require that the presented identity evidence be validated and verified through organizational-defined methods of validation and verification?	5
Identification & Authentication	In-Person Validation & Verification	IAC-28.4	Mechanisms exist to require that the validation and verification of identity evidence be conducted in person before a designated registration authority.	- In-person validation of government-issued photograph identification		Does the organization require that the validation and verification of identity evidence be conducted in person before a designated registration authority?	5
Identification & Authentication	Address Confirmation	IAC-28.5	Mechanisms exist to require that a notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital).			Does the organization require that a notice of proofing be delivered through an out-of-band channel to verify the user's address (physical or digital)?	1
Identification & Authentication	Attribute-Based Access Control (ABAC)	IAC-29	Mechanisms exist to enforce Attribute-Based Access Control (ABAC) for policy-driven, dynamic authorizations that supports the secure sharing of information.	- NIST Special Publication 800-162		Does the organization enforce Attribute-Based Access Control (ABAC) to enable policy-driven, dynamic authorizations and supports the secure sharing of information?	5
Incident Response	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and privacy-related incidents.			Does the organization facilitate the implementation of incident response controls?	9
Incident Response	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	- ITIL Infrastructure Library - Incident and problem management	E-IRO-03	Does the organization's incident handling processes cover preparation, detection and analysis, containment, eradication and recovery?	10
Incident Response	Automated Incident Handling Processes	IRO-02.1	Automated mechanisms exist to support the incident handling process.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization use automated mechanisms to support the incident handling process?	1
Incident Response	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.			Does the organization prevent identity theft from occurring?	5
Incident Response	Dynamic Reconfiguration	IRO-02.3	Automated mechanisms exist to dynamically reconfigure information system components as part of the incident response capability.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization dynamically reconfigure information system components as part of the incident response capability?	5

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Incident Response	Continuity of Operations	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.			Does the organization identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions?	5
Incident Response	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.			Does the organization coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses?	5
Incident Response	Automatic Disabling of System	IRO-02.6	Mechanisms exist to automatically disable systems, upon detection of a possible incident that meets organizational criteria, which allows for forensic analysis to be performed.			Does the organization automatically disable systems involved in an incident that meet organizational criteria to be automatically disabled upon detection?	6
Incident Response	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	- Indicators of Compromise (IoC) - Incident Response Plan (IRP) - Strake (https://9yahds.com/) - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)	E-IRO-02	Does the organization define specific Indicators of Compromise (IOC) that identify the potential impact of likely cybersecurity events?	8
Incident Response	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	- Incident Response Plan (IRP) - Hard copy of IRP	E-IRO-01	Does the organization maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders?	9
Incident Response	Data Breach	IRO-04.1	Mechanisms exist to address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations.			Does the organization address data breaches, or other incidents involving the unauthorized disclosure of sensitive or regulated data, according to applicable laws, regulations and contractual obligations?	8
Incident Response	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.		E-IRO-07	Does the organization regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary?	8
Incident Response	Continuous Incident Response Improvements	IRO-04.3	Mechanisms exist to use qualitative and quantitative data from incident response testing to: •Determine the effectiveness of incident response processes; •Continuously improve incident response processes; and •Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.			Does the organization use qualitative and quantitative data from incident response testing to: •Determine the effectiveness of incident response processes; •Continuously improve incident response processes; and •Provide incident response measures and metrics that are accurate, consistent, and in	3
Incident Response	Incident Response Training	IRO-05	Mechanisms exist to train personnel in their incident response roles and responsibilities.	- ITIL Infrastructure Library - Incident and problem management - Incident Response Plan (IRP) - Strake (https://9yahds.com/)	E-IRO-05 E-IRO-06	Does the organization train personnel in their incident response roles and responsibilities?	9
Incident Response	Simulated Incidents	IRO-05.1	Mechanisms exist to incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.			Does the organization incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations?	5
Incident Response	Automated Incident Response Training Environments	IRO-05.2	Automated mechanisms exist to provide a more thorough and realistic incident response training environment.			Does the organization provide a more thorough and realistic incident response training environment?	5
Incident Response	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	- Strake (https://9yahds.com/) - "Table Top" incident response exercises (rock drills) - "Red team vs blue team" exercises - EICAR test file antimalware detection and response exercises	E-IRO-04	Does the organization formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities?	9
Incident Response	Coordination with Related Plans	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.			Does the organization coordinate incident response testing with organizational elements responsible for related plans?	7

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Incident Response	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and privacy incident response operations.	- Full-time employees only		Does the organization establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and privacy incident response operations?	9
Incident Response	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	- Chain of custody procedures - Encase - Forensic Tool Kit (FTK)		Does the organization perform digital forensics and maintain the integrity of the chain of custody?	9
Incident Response	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and privacy incidents to internal stakeholders all the way through the resolution of the incident.	- Incident Response Plan (IRP) - Strake (https://9yahds.com/)	E-IRO-03	Does the organization document, monitor and report cybersecurity and privacy incidents?	8
Incident Response	Automated Tracking, Data Collection & Analysis	IRO-09.1	Automated mechanisms exist to assist in the tracking, collection and analysis of information from actual and potential cybersecurity and privacy incidents.	- Strake (https://9yahds.com/)		Does the organization use automated mechanisms to assist in the tracking, collection and analysis of information from actual and potential cybersecurity and privacy incidents?	1
Incident Response	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.			Does the organization report incidents: • Internally to organizational incident response personnel within organization-defined time-periods; and • Externally to regulatory authorities and affected parties, as necessary?	9
Incident Response	Automated Reporting	IRO-10.1	Automated mechanisms exist to assist in the reporting of cybersecurity and privacy incidents.	- Strake (https://9yahds.com/)		Does the organization use automated mechanisms to assist in the reporting of cybersecurity and privacy incidents?	9
Incident Response	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.			Does the organization report sensitive/regulated data incidents in a timely manner?	9
Incident Response	Vulnerabilities Related To Incidents	IRO-10.3	Mechanisms exist to report system vulnerabilities associated with reported cybersecurity and privacy incidents to organization-defined personnel or roles.			Does the organization report system vulnerabilities associated with reported cybersecurity and privacy incidents to organization-defined personnel or roles?	8
Incident Response	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.			Does the organization provide cybersecurity and privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident?	7
Incident Response	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of systems for the handling and reporting of actual and potential cybersecurity and privacy incidents.	- ITIL Infrastructure Library - Incident and problem management		Does the organization provide incident response advice and assistance to users of systems for the handling and reporting of actual and potential cybersecurity and privacy incidents?	5
Incident Response	Automation Support of Availability of Information / Support	IRO-11.1	Automated mechanisms exist to increase the availability of incident response-related information and support.			Does the organization use automated mechanisms to increase the availability of incident response-related information and support?	1
Incident Response	Coordination With External Providers	IRO-11.2	Mechanisms exist to establish a direct, cooperative relationship between the organization's incident response capability and external service providers.			Does the organization establish a direct, cooperative relationship between the organization's incident response capability and external service providers?	5
Incident Response	Information Spillage Response	IRO-12	Mechanisms exist to respond to sensitive information spills.			Does the organization respond to sensitive information spills?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Incident Response	Responsible Personnel	IRO-12.1	Mechanisms exist to formally assign personnel or roles with responsibility for responding to sensitive information spills.			Does the organization formally assign personnel or roles with responsibility for responding to sensitive information spills?	8
Incident Response	Training	IRO-12.2	Mechanisms exist to ensure incident response training material provides coverage for sensitive information spillage response.			Does the organization ensure incident response training material provides coverage for sensitive information spillage response?	8
Incident Response	Post-Spill Operations	IRO-12.3	Mechanisms exist to ensure that organizational personnel impacted by sensitive information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions.			Does the organization ensure that organizational personnel impacted by sensitive information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions?	8
Incident Response	Exposure to Unauthorized Personnel	IRO-12.4	Mechanisms exist to address security safeguards for personnel exposed to sensitive information that is not within their assigned access authorizations.			Does the organization address security safeguards for personnel exposed to sensitive information that is not within their assigned access authorizations?	8
Incident Response	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and privacy incidents to reduce the likelihood or impact of future incidents.		E-IRO-08	Does the organization incorporate lessons learned from analyzing and resolving cybersecurity and privacy incidents to reduce the likelihood or impact of future incidents?	8
Incident Response	Regulatory & Law Enforcement Contacts	IRO-14	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.			Does the organization maintain incident response contacts with applicable regulatory and law enforcement agencies?	9
Incident Response	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	- Separate network with "sacrificial" systems where potential malware can be evaluated without impacting the production network.		Does the organization utilize a detonation chamber capability for incident response operations?	5
Incident Response	Public Relations & Reputation Repair	IRO-16	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's reputation.			Does the organization proactively manage public relations associated with an incident and employ appropriate measures to repair the reputation of the organization?	6
Information Assurance	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and privacy assessment and authorization controls.	- Information Assurance (IA) program - VisibleOps security management	E-IAO-01	Does the organization facilitate the implementation of cybersecurity and privacy assessment and authorization controls?	10
Information Assurance	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.		E-AST-02	Does the organization establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly and indirectly impacts the confidentiality, integrity, availability and safety of the data and systems under review?	9
Information Assurance	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and 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.	- Information Assurance (IA) program - VisibleOps security management - Information Assurance Program (IAP)		Does the organization formally assess the cybersecurity and 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?	10
Information Assurance	Assessor Independence	IAO-02.1	Mechanisms exist to ensure assessors or assessment teams have the appropriate independence to conduct cybersecurity and privacy control assessments.	- Information Assurance (IA) program - VisibleOps security management		Does the organization ensure assessors or assessment teams have the appropriate independence to conduct cybersecurity and privacy control assessments?	9
Information Assurance	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: • Statutory, regulatory and contractual compliance obligations; • Monitoring capabilities; • Mobile devices; • Databases;	- Information Assurance (IA) program - VisibleOps security management - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker		Does the organization conduct specialized assessments for: • Statutory, regulatory and contractual compliance obligations; • Monitoring capabilities; • Mobile devices; • Databases;	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Information Assurance	Third-Party Assessments	IAO-02.3	Mechanisms exist to accept and respond to the results of external assessments that are performed by impartial, external organizations.	- Audit steering committee - Information Assurance (IA) program - VisibleOps security management		Does the organization accept and respond to the results of external assessments that are performed by impartial, external organizations?	9
Information Assurance	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.			Does the organization produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions?	7
Information Assurance	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	- Information Assurance (IA) program - VisibleOps security management	E-TDA-14	Does the organization generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influencing inputs, entities, systems, applications and processes, providing a historical record of the data and its origins?	7
Information Assurance	Plan / Coordinate with Other Organizational Entities	IAO-03.1	Mechanisms exist to plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations.	- Audit steering committee - Information Assurance (IA) program - VisibleOps security management - Information Assurance Program (IAP)		Does the organization plan and coordinate Information Assurance Program (IAP) activities with affected stakeholders before conducting such activities in order to reduce the potential impact on operations?	5
Information Assurance	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	- Information Assurance (IA) program - VisibleOps security management		Does the organization protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract?	7
Information Assurance	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Test and Evaluation (ST&E) plan to identify and remediate flaws during development.	- Information Assurance (IA) program - VisibleOps security management - Security Test & Evaluation (ST&E)		Does the organization require system developers and integrators to create and execute a Security Test and Evaluation (ST&E) plan to identify and remediate flaws during development?	10
Information Assurance	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	- Information Assurance (IA) program - VisibleOps security management - Plan of Action & Milestones (POA&M)		Does the organization use a Plan of Action and Milestones (POA&M), or similar mechanisms, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities?	9
Information Assurance	Plan of Action & Milestones (POA&M) Automation	IAO-05.1	Automated mechanisms exist to help ensure the Plan of Action and Milestones (POA&M), or similar risk register, is accurate, up-to-date and readily-available.	- Governance, Risk & Compliance (GRC)		Does the organization automate Plan of Action and Milestones (POA&M), or similar a risk register, ensure it is accurate, up-to-date and readily-available?	2
Information Assurance	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity and privacy controls.	- Information Assurance (IA) program - VisibleOps security management - Information Assurance Program (IAP)		Does the organization perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity and privacy controls?	8
Information Assurance	Security Authorization	IAO-07	Mechanisms exist to ensure systems, projects and services are officially authorized prior to "go live" in a production environment.	- Information Assurance (IA) program - VisibleOps security management		Does the organization ensure systems, projects and services are officially authorized prior to "go live" in a production environment?	10
Maintenance	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.		E-MNT-02 E-MNT-04	Does the organization develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise?	9
Maintenance	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service.	- VisibleOps security management	E-MNT-04	Does the organization conduct controlled maintenance activities throughout the lifecycle of the system, application or service?	10
Maintenance	Automated Maintenance Activities	MNT-02.1	Automated mechanisms exist to schedule, conduct and document maintenance and repairs.			Does the organization schedule, conduct and document maintenance and repairs?	5

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Maintenance	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for systems within a defined Recovery Time Objective (RTO).		E-MNT-04	Does the organization obtain maintenance support and/or spare parts for systems within a defined Recovery Time Objective (RTO)?	9
Maintenance	Preventative Maintenance	MNT-03.1	Mechanisms exist to perform preventive maintenance on critical systems, applications and services.		E-MNT-04	Does the organization perform preventive maintenance on critical systems, applications and services?	5
Maintenance	Predictive Maintenance	MNT-03.2	Mechanisms exist to perform predictive maintenance on critical systems, applications and services.			Does the organization perform predictive maintenance on critical systems, applications and services?	5
Maintenance	Automated Support For Predictive Maintenance	MNT-03.3	Automated mechanisms exist to transfer predictive maintenance data to a computerized maintenance management system.			Does the organization transfer predictive maintenance data to a computerized maintenance management system?	5
Maintenance	Maintenance Tools	MNT-04	Mechanisms exist to control and monitor the use of system maintenance tools.	- VisibleOps security management		Does the organization control and monitor the use of system maintenance tools?	5
Maintenance	Inspect Tools	MNT-04.1	Mechanisms exist to inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.			Does the organization inspect maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications?	5
Maintenance	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.			Does the organization check media containing diagnostic and test programs for malicious code before the media are used?	5
Maintenance	Prevent Unauthorized Removal	MNT-04.3	Mechanisms exist to prevent or control the removal of equipment undergoing maintenance that containing organizational information.			Does the organization prevent or control the removal of equipment undergoing maintenance that containing organizational information?	9
Maintenance	Restrict Tool Usage	MNT-04.4	Automated mechanisms exist to restrict the use of maintenance tools to authorized maintenance personnel and/or roles.			Does the organization restrict the use of maintenance tools to authorized maintenance personnel and/or roles?	5
Maintenance	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.			Does the organization authorize, monitor and control remote, non-local maintenance and diagnostic activities?	9
Maintenance	Auditing Remote Maintenance	MNT-05.1	Mechanisms exist to audit remote, non-local maintenance and diagnostic sessions, as well as review the maintenance action performed during remote maintenance sessions.			Does the organization audit remote, non-local maintenance and diagnostic sessions and review the maintenance records of the sessions?	9
Maintenance	Remote Maintenance Notifications	MNT-05.2	Mechanisms exist to require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time).			Does the organization require maintenance personnel to notify affected stakeholders when remote, non-local maintenance is planned (e.g., date/time)?	9
Maintenance	Remote Maintenance Cryptographic Protection	MNT-05.3	Cryptographic mechanisms exist to protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications.			Does the organization cryptographically protect the integrity and confidentiality of remote, non-local maintenance and diagnostic communications?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Maintenance	Remote Maintenance Disconnect Verification	MNT-05.4	Mechanisms exist to provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated.			Does the organization provide remote disconnect verification to ensure remote, non-local maintenance and diagnostic sessions are properly terminated?	9
Maintenance	Remote Maintenance Pre-Approval	MNT-05.5	Mechanisms exist to require maintenance personnel to obtain pre-approval and scheduling for remote, non-local maintenance sessions.	- VisibleOps security management		Does the organization require maintenance personnel to obtain pre-approval and scheduling for remote, non-local maintenance sessions?	7
Maintenance	Remote Maintenance Comparable Security & Sanitization	MNT-05.6	Mechanisms exist to require systems performing remote, non-local maintenance and / or diagnostic services implement a security capability comparable to the capability implemented on the system being serviced.			Does the organization require systems performing remote, non-local maintenance and / or diagnostic services implement a security capability comparable to the capability implemented on the system being serviced?	5
Maintenance	Separation of Maintenance Sessions	MNT-05.7	Mechanisms exist to protect maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from other network sessions.			Does the organization protect maintenance sessions through replay-resistant sessions that are physically or logically separated communications paths from other network sessions?	1
Maintenance	Authorized Maintenance Personnel	MNT-06	Mechanisms exist to maintain a current list of authorized maintenance organizations or personnel.	- VisibleOps security management		Does the organization maintain a current list of authorized maintenance organizations or personnel?	9
Maintenance	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	- VisibleOps security management	E-MNT-01	Does the organization ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated?	7
Maintenance	Non-System Related Maintenance	MNT-06.2	Mechanisms exist to ensure that non-escorted personnel performing non-IT maintenance activities in the physical proximity of IT systems have required access authorizations.			Does the organization ensure that non-escorted personnel performing non-IT maintenance activities in the physical proximity of IT systems have required access authorizations?	5
Maintenance	Maintain Configuration Control During Maintenance	MNT-07	Mechanisms exist to maintain proper physical security and configuration control over technology assets awaiting service or repair.			Does the organization maintain proper physical security and configuration control over technology assets awaiting service or repair?	8
Maintenance	Field Maintenance	MNT-08	Mechanisms exist to securely conduct field maintenance on geographically deployed assets.			Does the organization securely conduct field maintenance on geographically deployed assets?	8
Maintenance	Off-Site Maintenance	MNT-09	Mechanisms exist to ensure off-site maintenance activities are conducted securely and the asset(s) undergoing maintenance actions are secured during physical transfer and storage while off-site.			Does the organization ensure off-site maintenance activities are conducted securely and the asset(s) undergoing maintenance actions are secured during physical transfer and storage while off-site?	8
Maintenance	Maintenance Validation	MNT-10	Mechanisms exist to validate maintenance activities were appropriately performed according to the work order and that security controls are operational.			Does the organization validate maintenance activities were appropriately performed according to the work order and that security controls are operational?	6
Maintenance	Maintenance Monitoring	MNT-11	Mechanisms exist to maintain situational awareness of the quality and reliability of systems and components through tracking maintenance activities and component failure rates.			Does the organization maintain situational awareness of the quality and reliability of systems and components through tracking maintenance activities and component failure rates?	6
Mobile Device Management	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of mobile device management controls.			Does the organization develop, govern & update procedures to facilitate the implementation of mobile device management controls?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Mobile Device Management	Access Control For Mobile Devices	MDM-02	Mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational systems.			Do access control mechanisms for mobile devices enforce requirements for the connection of mobile devices to organizational systems?	9
Mobile Device Management	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.			Are cryptographic mechanisms utilized to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption?	9
Mobile Device Management	Mobile Device Tampering	MDM-04	Mechanisms exist to protect mobile devices from tampering through inspecting devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network.			Does the organization protect mobile devices from tampering through inspecting devices returning from locations that the organization deems to be of significant risk, prior to the device being connected to the organization's network?	9
Mobile Device Management	Remote Purging	MDM-05	Mechanisms exist to remotely purge selected information from mobile devices.			Does the organization remotely purge selected information from mobile devices?	9
Mobile Device Management	Personally-Owned Mobile Devices	MDM-06	Mechanisms exist to restrict the connection of personally-owned, mobile devices to organizational systems and networks.			Does the organization restrict the connection of personally-owned, mobile devices to organizational systems and networks?	8
Mobile Device Management	Organization-Owned Mobile Devices	MDM-07	Mechanisms exist to prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store.			Does the organization prohibit the installation of non-approved applications or approved applications not obtained through the organization-approved application store?	8
Mobile Device Management	Mobile Device Data Retention Limitations	MDM-08	Mechanisms exist to limit data retention on mobile devices to the smallest usable dataset and timeframe.			Does the organization limit data retention on mobile devices to the smallest usable dataset and timeframe?	7
Mobile Device Management	Mobile Device Geofencing	MDM-09	Mechanisms exist to restrict the functionality of mobile devices based on geographic location.			Does the organization restrict the functionality of mobile devices based on geographic location?	7
Mobile Device Management	Separate Mobile Device Profiles	MDM-10	Mechanisms exist to enforce a separate device workspace on applicable mobile devices to separate work-related and personal-related applications and data.			Does the organization enforce a separate device workspace on applicable mobile devices to separate work-related and personal-related applications and data?	7
Mobile Device Management	Restricting Access To Authorized Devices	MDM-11	Mechanisms exist to restrict the connectivity of unauthorized mobile devices from communicating with systems, applications and services.			Does the organization restrict the connectivity of unauthorized mobile devices from communicating with systems, applications and services?	8
Network Security	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization develop, govern & update procedures to facilitate the implementation of network security controls?	10
Network Security	Zero Trust Architecture (ZTA)	NET-01.1	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.			Does the organization treat all users as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized?	8
Network Security	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.		E-DCH-03 E-DCH-04 E-DCH-05	Does the organization 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?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Network Security	Denial of Service (DoS) Protection	NET-02.1	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.			Does the organization protect against or limit the effects of Denial of Service (DoS) attacks?	9
Network Security	Guest Networks	NET-02.2	Mechanisms exist to implement and manage a secure guest network.			Does the organization implement and manage a secure guest network?	6
Network Security	Cross Domain Solution (CDS)	NET-02.3	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.			Does the organization implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains?	6
Network Security	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.			Are boundary protection mechanisms utilized to monitor and control communications at the external network boundary and at key internal boundaries within the network?	10
Network Security	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its systems.			Does the organization limit the number of concurrent external network connections to its systems?	9
Network Security	External Telecommunications Services	NET-03.2	Mechanisms exist to maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface.	- Outbound content filtering		Does the organization maintain a managed interface for each external telecommunication service that protects the confidentiality and integrity of the information being transmitted across each interface?	7
Network Security	Prevent Discovery of Internal Information	NET-03.3	Mechanisms exist to prevent the public disclosure of internal network information.			Does the organization prevent the public disclosure of internal address information?	7
Network Security	Personal Data (PD)	NET-03.4	Mechanisms exist to apply network-based processing rules to data elements of Personal Data (PD).	- Data Loss Prevention (DLP)		Does the organization apply network-based processing rules to data elements of Personal Data (PD)?	7
Network Security	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces.			Does the organization prevent the unauthorized exfiltration of sensitive/regulated data across managed interfaces?	5
Network Security	Dynamic Isolation & Segregation (Sandboxing)	NET-03.6	Automated mechanisms exist to dynamically isolate (e.g., sandbox) untrusted components during runtime, where the component is isolated in a fault-contained environment but it can still collaborate with the application.			Does the organization dynamically isolate (e.g., sandbox) untrusted components during runtime, where the component is isolated in a fault-contained environment but it can still collaborate with the application?	5
Network Security	Isolation of Information System Components	NET-03.7	Mechanisms exist to employ boundary protections to isolate systems, services and processes that support critical missions and/or business functions.			Does the organization employ boundary protections to isolate systems, services and process that support critical missions and/or business functions?	5
Network Security	Separate Subnet for Connecting to Different Security Domains	NET-03.8	Mechanisms exist to implement separate network addresses (e.g., different subnets) to connect to systems in different security domains.			Does the organization implement separate network addresses (e.g., different subnets) to connect to systems in different security domains?	5
Network Security	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)	E-AST-12 E-AST-19	Does the organization design, implement and review firewall and router configurations to restrict connections between untrusted networks and internal systems?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Network Security	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).		E-AST-12 E-AST-19	Does the organization configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception)?	10
Network Security	Object Security Attributes	NET-04.2	Mechanisms exist to associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions.	- NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization associate security attributes with information, source and destination objects to enforce defined information flow control configurations as a basis for flow control decisions?	5
Network Security	Content Check for Encrypted Data	NET-04.3	Mechanisms exist to prevent encrypted data from bypassing content-checking mechanisms.			Does the organization prevent encrypted data from bypassing content-checking mechanisms?	4
Network Security	Embedded Data Types	NET-04.4	Mechanisms exist to enforce limitations on embedding data within other data types.	- Prevent exfiltration through steganography		Does the organization enforce limitations on embedding data within other data types?	2
Network Security	Metadata	NET-04.5	Mechanisms exist to enforce information flow controls based on metadata.			Does the organization enforce information flow controls based on metadata?	2
Network Security	Human Reviews	NET-04.6	Mechanisms exist to enforce the use of human reviews for Access Control Lists (ACLs) and similar rulesets on a routine basis.		E-AST-12	Does the organization enforce the use of human reviews for Access Control Lists (ACLs) and similar rulesets on a routine basis?	9
Network Security	Security Policy Filters	NET-04.7	Automated mechanisms exist to enforce information flow control using security policy filters as a basis for flow control decisions.			Does the organization enforce information flow control using security policy filters as a basis for flow control decisions?	5
Network Security	Data Type Identifiers	NET-04.8	Automated mechanisms exist to utilize data type identifiers to validate data essential for information flow decisions when transferring information between different security domains.			Does the organization utilize data type identifiers to validate data essential for information flow decisions when transferring information between different security domains?	5
Network Security	Decomposition Into Policy-Related Subcomponents	NET-04.9	Automated mechanisms exist to decompose information into policy-relevant subcomponents for submission to policy enforcement mechanisms, when transferring information between different security domains.			Does the organization decompose information into policy-relevant subcomponents for submission to policy enforcement mechanisms, when transferring information between different security domains?	5
Network Security	Detection of Unsanctioned Information	NET-04.10	Automated mechanisms exist to implement security policy filters requiring fully enumerated formats that restrict data structure and content, when transferring information between different security domains.			Does the organization implement security policy filters requiring fully enumerated formats that restrict data structure and content, when transferring information between different security domains?	5
Network Security	Approved Solutions	NET-04.11	Automated mechanisms exist to examine information for the presence of unsanctioned information and prohibits the transfer of such information, when transferring information between different security domains.			Does the organization examine information for the presence of unsanctioned information and prohibits the transfer of such information, when transferring information between different security domains?	5
Network Security	Cross Domain Authentication	NET-04.12	Automated mechanisms exist to uniquely identify and authenticate source and destination points for information transfer.			Does the organization uniquely identify and authenticate source and destination points for information transfer?	5
Network Security	Metadata Validation	NET-04.13	Automated mechanisms exist to apply security and/or privacy filters on metadata.			Does the organization apply security and/or privacy filters on metadata?	2

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Network Security	System Interconnections	NET-05	Mechanisms exist to authorize connections from systems to other systems using Interconnection Security Agreements (ISAs) that document, for each interconnection, the interface characteristics, cybersecurity and privacy requirements and the nature of the information communicated.	- VisibleOps security management		Does the organization authorize connections from systems to other systems using Interconnection Security Agreements (ISAs) that document, for each interconnection, the interface characteristics, cybersecurity and privacy requirements and the nature of the information communicated?	9
Network Security	External System Connections	NET-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.			Does the organization prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device?	8
Network Security	Internal System Connections	NET-05.2	Mechanisms exist to control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated.			Does the organization control internal system connections through authorizing internal connections of systems and documenting, for each internal connection, the interface characteristics, security requirements and the nature of the information communicated?	7
Network Security	Network Segmentation	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	- Subnetting - VLANs		Does the organization logically or physically segment information flows to accomplish network segmentation?	10
Network Security	Security Management Subnets	NET-06.1	Mechanisms exist to implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system.			Does the organization implement security management subnets to isolate security tools and support components from other internal system components by implementing separate subnetworks with managed interfaces to other components of the system?	9
Network Security	Virtual Local Area Network (VLAN) Separation	NET-06.2	Mechanisms exist to enable Virtual Local Area Networks (VLANs) to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems.	- Virtual Local Area Network (VLAN)		Does the organization enable Virtual Local Area Networks (VLANs) to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems?	9
Network Security	Sensitive / Regulated Data Enclave (Secure Zone)	NET-06.3	Mechanisms exist to implement segmentation controls to restrict inbound and outbound connectivity for sensitive / regulated data enclaves (secure zones).			Does the organization implement segmentation controls to restrict inbound and outbound connectivity for sensitive / regulated data enclaves (secure zones)?	10
Network Security	Segregation From Enterprise Services	NET-06.4	Mechanisms exist to isolate sensitive / regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware, patch management, etc.) to those isolated network segments.			Does the organization isolate sensitive / regulated data enclaves (secure zones) from corporate-provided IT resources by providing enclave-specific IT services (e.g., directory services, DNS, NTP, ITAM, antimalware, patch management, etc.) to those isolated network segments?	4
Network Security	Direct Internet Access Restrictions	NET-06.5	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive / regulated data enclaves (secure zones).			Does the organization prohibit, or strictly-control, Internet access from sensitive / regulated data enclaves (secure zones)?	6
Network Security	Remote Session Termination	NET-07	Mechanisms exist to terminate remote sessions at the end of the session or after an organization-defined time period of inactivity.			Does the organization terminate remote sessions at the end of the session or after an organization-defined time period of inactivity?	8
Network Security	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.			Are Network Intrusion Detection / Prevention Systems (NIDS/NIPS) used to detect and/or prevent intrusions into the network?	9
Network Security	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	- Architectural review board - System Security Plan (SSP)		Does the organization monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks?	8
Network Security	Wireless Intrusion Detection / Prevention Systems (WIDS / WIPS)	NET-08.2	Mechanisms exist to monitor wireless network segments to implement Wireless Intrusion Detection / Prevention Systems (WIDS/WIPS) technologies.			Does the organization monitor wireless network segments to implement Wireless Intrusion Detection / Prevention Systems (WIDS/WIPS) technologies?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Network Security	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	- PKI for non-repudiation		Does the organization protect the authenticity and integrity of communications sessions?	8
Network Security	Invalidate Session Identifiers at Logout	NET-09.1	Automated mechanisms exist to invalidate session identifiers upon user logout or other session termination.			Does the organization invalidate session identifiers upon user logout or other session termination?	5
Network Security	Unique System-Generated Session Identifiers	NET-09.2	Automated mechanisms exist to generate and recognize unique session identifiers for each session.			Does the organization automatically generate and recognize unique session identifiers for each session?	3
Network Security	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.			Does the organization ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution?	10
Network Security	Architecture & Provisioning for Name / Address Resolution Service	NET-10.1	Mechanisms exist to ensure systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement internal/external role separation.			Does the organization ensure systems that collectively provide Domain Name Service (DNS) resolution service are fault-tolerant and implement internal/external role separation?	9
Network Security	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-10.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.			Does the organization perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems?	9
Network Security	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.			Does the organization 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?	8
Network Security	Domain Registrar Security	NET-10.4	Mechanisms exist to lock the domain name registrar to prevent a denial of service caused by unauthorized deletion, transfer or other unauthorized modification of a domain's registration details.			Does the organization lock the domain name registrar to prevent a denial of service caused by unauthorized deletion, transfer or other unauthorized modification of a domain's registration details?	9
Network Security	Out-of-Band Channels	NET-11	Mechanisms exist to utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals.	- Signature delivery (courier service)		Does the organization utilize out-of-band channels for the electronic transmission of information and/or the physical shipment of system components or devices to authorized individuals?	9
Network Security	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.			Does the organization use strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks?	8
Network Security	Wireless Link Protection	NET-12.1	Mechanisms exist to protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered.			Does the organization protect external and internal wireless links from signal parameter attacks through monitoring for unauthorized wireless connections, including scanning for unauthorized wireless access points and taking appropriate action, if an unauthorized connection is discovered?	8
Network Security	End-User Messaging Technologies	NET-12.2	Mechanisms exist to prohibit the transmission of unprotected sensitive/regulated data by end-user messaging technologies.	- Acceptable Use Policy (AUP) - Data Loss Prevention (DLP)		Does the organization prohibit the transmission of unprotected sensitive/regulated data by end-user messaging technologies?	9
Network Security	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.			Does the organization protect the confidentiality, integrity and availability of electronic messaging communications?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Network Security	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.		E-NET-03	Does the organization define, control and review organization-approved, secure remote access methods?	10
Network Security	Automated Monitoring & Control	NET-14.1	Automated mechanisms exist to monitor and control remote access sessions.			Does the organization use automated mechanisms to monitor and control remote access sessions?	1
Network Security	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).			Does the organization cryptographically protect the confidentiality and integrity of remote access sessions (e.g., VPN)?	9
Network Security	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).			Does the organization route all remote accesses through managed network access control points (e.g., VPN concentrator)?	9
Network Security	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.			Does the organization restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs?	8
Network Security	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to systems and data for remote workers.		E-NET-03	Does the organization define secure telecommuting practices and govern remote access to systems and data for remote workers?	10
Network Security	Third-Party Remote Access Governance	NET-14.6	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.			Does the organization proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access?	8
Network Security	Endpoint Security Validation	NET-14.7	Mechanisms exist to validate software versions/patch levels and control remote devices connecting to corporate networks or storing and accessing organization information.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization validate software versions/patch levels and control remote devices connecting to corporate networks or storing and accessing organization information?	6
Network Security	Expeditious Disconnect / Disable Capability	NET-14.8	Mechanisms exist to provide the capability to expeditiously disconnect or disable a user's remote access session.			Does the organization provide the capability to expeditiously disconnect or disable a user's remote access session?	8
Network Security	Wireless Networking	NET-15	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.			Does the organization control authorized wireless usage and monitor for unauthorized wireless access?	9
Network Security	Authentication & Encryption	NET-15.1	Mechanisms exist to protect wireless access through authentication and strong encryption.			Are authentication and cryptographic mechanisms used to protect wireless access?	9
Network Security	Disable Wireless Networking	NET-15.2	Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users.			Does the organization disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users?	5
Network Security	Restrict Configuration By Users	NET-15.3	Mechanisms exist to identify and explicitly authorize users who are allowed to independently configure wireless networking capabilities.			Does the organization identify and explicitly authorize users who are allowed to independently configure wireless networking capabilities?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Network Security	Wireless Boundaries	NET-15.4	Mechanisms exist to confine wireless communications to organization-controlled boundaries.			Does the organization confine wireless communications to organization-controlled boundaries?	5
Network Security	Rogue Wireless Detection	NET-15.5	Mechanisms exist to test for the presence of Wireless Access Points (WAPs) and identify all authorized and unauthorized WAPs within the facility(ies).		E-NET-02	Does the organization test for the presence of Wireless Access Points (WAPs) and identify all authorized and unauthorized WAPs within the facility(ies)?	8
Network Security	Intranets	NET-16	Mechanisms exist to establish trust relationships with other organizations owning, operating, and/or maintaining intranet systems, allowing authorized individuals to: • Access the intranet from external systems; and • Process, store, and/or transmit organization-controlled information using the external systems.			Does the organization establish trust relationships with other organizations owning, operating, and/or maintaining intranet systems, allowing authorized individuals to: • Access the intranet from external systems; and • Process, store, and/or transmit organization-controlled information using the external systems?	8
Network Security	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	- Data Loss Prevention (DLP)		Is Data Loss Prevention (DLP) used to protect sensitive information as it is stored, transmitted and processed?	8
Network Security	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.		E-NET-01	Does the organization force Internet-bound network traffic through a proxy device for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites?	9
Network Security	Route Traffic to Proxy Servers	NET-18.1	Mechanisms exist to route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces.		E-NET-01	Does the organization route internal communications traffic to external networks through organization-approved proxy servers at managed interfaces?	9
Network Security	Visibility of Encrypted Communications	NET-18.2	Mechanisms exist to configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms.			Does the organization configure the proxy to make encrypted communications traffic visible to monitoring tools and mechanisms?	5
Network Security	Route Privileged Network Access	NET-18.3	Automated mechanisms exist to route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.			Does the organization route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing?	1
Physical & Environmental Security	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.		E-PES-01	Does the organization facilitate the operation of physical and environmental protection controls?	9
Physical & Environmental Security	Site Security Plan (SitePlan)	PES-01.1	Mechanisms exist to document a Site Security Plan (SitePlan) for each server and communications room to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.		E-PES-04	Does the organization document a Site Security Plan (SitePlan) for each server and communications room to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats?	4
Physical & Environmental Security	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).		E-PES-03	Does the organization maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible)?	7
Physical & Environmental Security	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.		E-PES-03	Does the organization authorize physical access to facilities based on the position or role of the individual?	9
Physical & Environmental Security	Dual Authorization for Physical Access	PES-02.2	Mechanisms exist to enforce a "two-person rule" for physical access by requiring two authorized individuals with separate access cards, keys or PINs, to access highly-sensitive areas (e.g., safe, high-security cage, etc.).			Does the organization enforce a "two-person rule" for physical access by requiring two authorized individuals with separate access cards, keys or PINs, to access highly-sensitive areas (e.g., safe, high-security cage, etc.?)?	2

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Physical & Environmental Security	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	- Security guards - Verify individual access authorizations before granting access to the facility. - Control entry to the facility containing the system using physical access devices and/or guards.	E-PES-02	Does the organization enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible)?	10
Physical & Environmental Security	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.			Does the organization limit and monitor physical access through controlled ingress and egress points?	9
Physical & Environmental Security	Lockable Physical Casings	PES-03.2	Physical access control mechanisms exist to protect system components from unauthorized physical access (e.g., lockable physical casings).	- CCTV - Lockable server/network racks - Logged access badges to access server rooms		Does the organization protect system components from unauthorized physical access (e.g., lockable physical casings)?	5
Physical & Environmental Security	Physical Access Logs	PES-03.3	Physical access control mechanisms exist to generate a log entry for each access through controlled ingress and egress points.	- Visitor logbook - iLobby (https://goilobby.com/) - The Receptionist (https://thereceptionist.com/) - LobbyGuard (http://lobbyguard.com/)	E-PES-02	Does the organization generate a log entry for each access through controlled ingress and egress points?	6
Physical & Environmental Security	Access To Information Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical information systems or sensitive/regulated data, in addition to the physical access controls for the facility.			Does the organization enforce physical access to critical information systems or sensitive/regulated data, in addition to the physical access controls for the facility?	5
Physical & Environmental Security	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	- "clean desk" policy - Management spot checks		Are physical access controls designed and implemented for offices, rooms and facilities?	10
Physical & Environmental Security	Working in Secure Areas	PES-04.1	Physical security mechanisms exist to allow only authorized personnel access to secure areas.	- Visitor escorts		Does the organization allow only authorized personnel access to secure areas?	10
Physical & Environmental Security	Searches	PES-04.2	Physical access control mechanisms exist to inspect personnel and their personal effects (e.g., personal property ordinarily worn or carried by the individual, including vehicles) to prevent the unauthorized exfiltration of data and technology assets.			Does the organization inspect personnel and their personal effects (e.g., personal property ordinarily worn or carried by the individual, including vehicles) to prevent the unauthorized exfiltration of data and technology assets?	1
Physical & Environmental Security	Temporary Storage	PES-04.3	Physical access control mechanisms exist to temporarily store undelivered packages or deliveries in a dedicated, secure area (e.g., security cage, secure room) that is locked, access-controlled and monitored with surveillance cameras and/or security guards.			Does the organization temporarily store undelivered packages or deliveries in a dedicated, secure area (e.g., security cage, secure room) that is locked, access-controlled and monitored with surveillance cameras and/or security guards?	2
Physical & Environmental Security	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.			Does the organization monitor for, detect and respond to physical security incidents?	7
Physical & Environmental Security	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	- CCTV		Does the organization monitor physical intrusion alarms and surveillance equipment?	9
Physical & Environmental Security	Monitoring Physical Access To Information Systems	PES-05.2	Facility security mechanisms exist to monitor physical access to critical information systems or sensitive/regulated data, in addition to the physical access monitoring of the facility.			Does the organization monitor physical access to critical information systems or sensitive/regulated data, in addition to the physical access monitoring of the facility?	5
Physical & Environmental Security	Visitor Control	PES-06	Physical access control mechanisms exist to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).	- Visitor logbook - iLobby (https://goilobby.com/) - The Receptionist (https://thereceptionist.com/) - LobbyGuard (http://lobbyguard.com/)	E-PES-02	Does the organization identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible)?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Physical & Environmental Security	Distinguish Visitors from On-Site Personnel	PES-06.1	Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible.	- Visible badges for visitors that are different from organizational personnel		Does the organization easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible?	8
Physical & Environmental Security	Identification Requirement	PES-06.2	Physical access control mechanisms exist to requires at least one (1) form of government-issued photo identification to authenticate individuals before they can gain access to the facility.			Does the organization requires at least one (1) form of government-issued photo identification to authenticate individuals before they can gain access to the facility?	8
Physical & Environmental Security	Restrict Unescorted Access	PES-06.3	Physical access control mechanisms exist to restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access.			Does the organization restrict unescorted access to facilities to personnel with required security clearances, formal access authorizations and validate the need for access?	10
Physical & Environmental Security	Automated Records Management & Review	PES-06.4	Automated mechanisms exist to facilitate the maintenance and review of visitor access records.		E-PES-02	Does the organization facilitate the maintenance and review of visitor access records?	5
Physical & Environmental Security	Minimize Visitor Personal Data (PD)	PES-06.5	Mechanisms exist to minimize the collection of Personal Data (PD) contained in visitor access records.			Does the organization minimize the collection of Personal Data (PD) contained in visitor access records?	3
Physical & Environmental Security	Visitor Access Revocation	PES-06.6	Mechanisms exist to ensure visitor badges, or other issued identification, are surrendered before visitors leave the facility or are deactivated at a pre-determined time/date of expiration.			Does the organization ensure visitor badges, or other issued identification, are surrendered before visitors leave the facility or are deactivated at a pre-determined time/date of expiration?	7
Physical & Environmental Security	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.		E-PES-01	Does the organization protect power equipment and power cabling for the system from damage and destruction?	9
Physical & Environmental Security	Automatic Voltage Controls	PES-07.1	Facility security mechanisms exist to utilize automatic voltage controls for critical system components.			Does the organization utilize automatic voltage controls for critical system components?	8
Physical & Environmental Security	Emergency Shutoff	PES-07.2	Facility security mechanisms exist to shut off power in emergency situations by: • Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and • Protecting emergency power shutoff capability from unauthorized activation.			Does the organization shut off power in emergency situations by: • Placing emergency shutoff switches or devices in close proximity to systems or system components to facilitate safe and easy access for personnel; and • Protecting emergency power shutoff capability from unauthorized activation?	8
Physical & Environmental Security	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.			Does the organization protect supply long-term alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source?	8
Physical & Environmental Security	Emergency Lighting	PES-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.			Does the organization utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility?	7
Physical & Environmental Security	Water Damage Protection	PES-07.5	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	- Water leak sensors - Humidity sensors		Does the organization protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel?	8
Physical & Environmental Security	Automation Support for Water Damage Protection	PES-07.6	Facility security mechanisms exist to detect the presence of water in the vicinity of critical information systems and alert facility maintenance and IT personnel.			Does the organization detect the presence of water in the vicinity of critical information systems and alert facility maintenance and IT personnel?	5

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Physical & Environmental Security	Redundant Cabling	PES-07.7	Mechanisms exist to employ redundant power cabling paths that are physically separated to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged.			Does the organization employ redundant power cabling paths that are physically separated to ensure that power continues to flow in the event one of the cables is cut or otherwise damaged?	2
Physical & Environmental Security	Fire Protection	PES-08	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.		E-PES-01	Does the organization utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy. source?	7
Physical & Environmental Security	Fire Detection Devices	PES-08.1	Facility security mechanisms exist to utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire.			Does the organization utilize and maintain fire detection devices/systems that activate automatically and notify organizational personnel and emergency responders in the event of a fire?	9
Physical & Environmental Security	Fire Suppression Devices	PES-08.2	Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency responders.			Does the organization utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency responders?	3
Physical & Environmental Security	Automatic Fire Suppression	PES-08.3	Facility security mechanisms exist to employ an automatic fire suppression capability for critical information systems when the facility is not staffed on a continuous basis.			Does the organization employ an automatic fire suppression capability for critical information systems when the facility is not staffed on a continuous basis?	5
Physical & Environmental Security	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.		E-PES-01	Does the organization maintain and monitor temperature and humidity levels within the facility?	9
Physical & Environmental Security	Monitoring with Alarms / Notifications	PES-09.1	Facility security mechanisms exist to trigger an alarm or notification of temperature and humidity changes that be potentially harmful to personnel or equipment.			Does the organization trigger an alarm or notification of temperature and humidity changes that be potentially harmful to personnel or equipment?	8
Physical & Environmental Security	Delivery & Removal	PES-10	Physical security mechanisms exist to isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access.			Does the organization isolate information processing facilities from points such as delivery and loading areas and other points to avoid unauthorized access?	8
Physical & Environmental Security	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.			Does the organization utilize appropriate management, operational and technical controls at alternate work sites?	8
Physical & Environmental Security	Equipment Siting & Protection	PES-12	Physical security mechanisms exist to locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.			Does the organization locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access?	9
Physical & Environmental Security	Transmission Medium Security	PES-12.1	Physical security mechanisms exist to protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage.			Does the organization protect power and telecommunications cabling carrying data or supporting information services from interception, interference or damage?	9
Physical & Environmental Security	Access Control for Output Devices	PES-12.2	Physical security mechanisms exist to restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output.	- Printer management (print only when at the printer with proximity card or code)		Does the organization restrict access to printers and other system output devices to prevent unauthorized individuals from obtaining the output?	8
Physical & Environmental Security	Information Leakage Due To Electromagnetic Signals Emanations	PES-13	Facility security mechanisms exist to protect the system from information leakage due to electromagnetic signals emanations.			Does the organization protect the system from information leakage due to electromagnetic signals emanations?	5

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Physical & Environmental Security	Asset Monitoring and Tracking	PES-14	Physical security mechanisms exist to employ asset location technologies that track and monitor the location and movement of organization-defined assets within organization-defined controlled areas.	- RFID tagging		Does the organization employ asset location technologies that track and monitor the location and movement of organization-defined assets within organization-defined controlled areas?	6
Physical & Environmental Security	Electromagnetic Pulse (EMP) Protection	PES-15	Physical security mechanisms exist to employ safeguards against Electromagnetic Pulse (EMP) damage for systems and system components.	- EMP shielding (Faraday cages)		Does the organization employ safeguards against Electromagnetic Pulse (EMP) damage for systems and system components?	1
Physical & Environmental Security	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.			Does the organization mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component?	3
Physical & Environmental Security	Proximity Sensor	PES-17	Automated mechanisms exist to monitor physical proximity to robotic or autonomous platforms to reduce applied force or stop the operation when sensors indicate a potentially dangerous scenario.			Does the organization continuously monitor physical proximity to robotic or autonomous platforms to reduce applied force or stop the operation when sensors indicate a potentially dangerous scenario?	9
Physical & Environmental Security	On-Site Client Segregation	PES-18	Mechanisms exist to ensure client-specific Intellectual Property (IP) is isolated from other data when client-specific IP is processed or stored within multi-client workspaces.			Does the organization ensure client-specific Intellectual Property (IP) is isolated from other data when client-specific IP is processed or stored within multi-client workspaces?	6
Privacy	Privacy Program	PRI-01	Mechanisms exist to facilitate the implementation and operation of privacy controls.		E-GOV-02 E-GOV-08	Does the organization facilitate the implementation and operation of privacy controls?	10
Privacy	Chief Privacy Officer (CPO)	PRI-01.1	Mechanisms exist to appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.		E-HRS-08	Does the organization appoints a Chief Privacy Officer (CPO) or similar role, with the authority, mission, accountability and resources to coordinate, develop and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program?	3
Privacy	Privacy Act Statements	PRI-01.2	Mechanisms exist to provide additional formal notice to individuals from whom the information is being collected that includes: • Notice of the authority of organizations to collect Personal Data (PD); • Whether providing Personal Data (PD) is mandatory or optional; • The principal purpose or purposes for which the Personal Data (PD) is to be used;			Does the organization provide additional formal notice to individuals from whom the information is being collected that includes: • Notice of the authority of organizations to collect Personal Data (PD); • Whether providing Personal Data (PD) is mandatory or optional; • The principal purpose or purposes for which the Personal Data (PD) is to be used;	2
Privacy	Dissemination of Privacy Program Information	PRI-01.3	Mechanisms exist to: • Ensure that the public has access to information about organizational privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; • Ensure that organizational privacy practices are publicly available through organizational websites or otherwise; and			Does the organization: • Ensure that the public has access to information about organizational privacy activities and can communicate with its Chief Privacy Officer (CPO) or similar role; • Ensure that organizational privacy practices are publicly available through organizational websites or otherwise; and	5
Privacy	Data Protection Officer (DPO)	PRI-01.4	Mechanisms exist to appoint a Data Protection Officer (DPO): • Based on the basis of professional qualities; and • To be involved in all issues related to the protection of personal data.		E-HRS-10	Does the organization appoint a Data Protection Officer (DPO): • Based on the basis of professional qualities; and • To be involved in all issues related to the protection of personal data?	7
Privacy	Binding Corporate Rules (BCR)	PRI-01.5	Mechanisms exist to implement and manage Binding Corporate Rules (BCR) (e.g., data sharing agreement) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data.		E-PRI-05	Does the organization implement and manage Binding Corporate Rules (BCR) to legally-bind all parties engaged in a joint economic activity that contractually states enforceable rights on data subjects with regard to the processing of their personal data?	5
Privacy	Security of Personal Data	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.			Does the organization ensure Personal Data (PD) is protected by security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD?	7
Privacy	Limiting Personal Data Disclosures	PRI-01.7	Mechanisms exist to limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained.			Does the organization limit the disclosure of Personal Data (PD) to authorized parties for the sole purpose for which the PD was obtained?	7

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Privacy	Privacy Notice	PRI-02	Mechanisms exist to: • Make privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; • Ensure that privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language that meet all legal obligations; and		E-PRI-08	Does the organization: • Make privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary? • Ensure that privacy notices are clear and easy-to-understand, expressing information about Personal Data (PD) processing in plain language?	7
Privacy	Purpose Specification	PRI-02.1	Mechanisms exist to identify and document the purpose(s) for which Personal Data (PD) is collected, used, maintained and shared in its privacy notices.			Does the organization identify and document the purpose(s) for which Personal Data (PD) is collected, used, maintained and shared in its privacy notices?	7
Privacy	Automated Data Management Processes	PRI-02.2	Automated mechanisms exist to adjust data that is able to be collected, created, used, disseminated, maintained, retained and/or disclosed, based on updated data subject authorization(s).	The organization should identify and address obligations, including legal obligations, to the PD principals resulting from decisions made by the organization which are related to the PD principal based solely on automated processing of PD.		Does the organization use automated mechanisms to support records management of authorizing policies and procedures for Personal Data (PD)?	1
Privacy	Computer Matching Agreements (CMA)	PRI-02.3	Mechanisms exist to publish Computer Matching Agreements (CMA) on the public website of the organization.			Does the organization publish Computer Matching Agreements (CMA) on the public website of the organization?	1
Privacy	System of Records Notice (SORN)	PRI-02.4	Mechanisms exist to draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.			Does the organization draft, publish and keep System of Records Notices (SORN) updated in accordance with regulatory guidance.	1
Privacy	System of Records Notice (SORN) Review Process	PRI-02.5	Mechanisms exist to review all routine uses of data published in the System of Records Notices (SORN) to ensure continued accuracy and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.			Does the organization review all routine uses of data published in the System of Records Notices (SORN) to ensure continued accuracy and to ensure that routine uses continue to be compatible with the purpose for which the information was collected?	1
Privacy	Privacy Act Exemptions	PRI-02.6	Mechanisms exist to review all Privacy Act exemptions claimed for the System of Records Notices (SORN) to ensure they remain appropriate and accurate.			Does the organization review all Privacy Act exemptions claimed for the System of Records Notices (SORN) to ensure they remain appropriate and accurate?	1
Privacy	Real-Time or Layered Notice	PRI-02.7	Mechanisms exist to provide real-time and/or layered notice when Personal Data (PD) is collected that provides data subjects with a summary of key points or more detailed information that is specific to the organization's privacy notice.			Does the organization provide real-time and/or layered notice when Personal Data (PD) is collected that provides data subjects with a summary of key points or more detailed information that is specific to the organization's privacy notice?	2
Privacy	Choice & Consent	PRI-03	Mechanisms exist to authorize the processing of their Personal Data (PD) prior to its collection that: • Uses plain language and provide examples to illustrate the potential privacy risks of the authorization; and • Provides a means for users to decline the authorization.	- "opt in" vs "opt out" user selections		Does the organization authorize the processing of their Personal Data (PD) prior to its collection that: • Uses plain language and provide examples to illustrate the potential privacy risks of the authorization; and • Provides a means for users to decline the authorization?	7
Privacy	Tailored Consent	PRI-03.1	Mechanisms exist to allow data subjects to modify the use permissions to selected attributes of their Personal Data (PD).			Does the organization allow data subjects to modify the use permissions to selected attributes of their Personal Data (PD)?	1
Privacy	Just-In-Time Notice & Updated Consent	PRI-03.2	Mechanisms exist to present authorizations to process Personal Data (PD) in conjunction with the data action, when: • The original circumstances under which an individual gave consent have changed; or • A significant amount of time has passed since an individual gave consent.			Does the organization present authorizations to process Personal Data (PD) in conjunction with the data action, when: • The original circumstances under which an individual gave consent have changed; or • A significant amount of time has passed since an individual gave consent?	1
Privacy	Prohibition Of Selling or Sharing Personal Data (PD)	PRI-03.3	Mechanisms exist to prevent the sale or sharing of Personal Data (PD) when instructed by the data subject.			Does the organization prevent the sale or sharing of Personal Data (PD) when instructed by the data subject?	5
Privacy	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to the processing of their Personal Data (PD).			Does the organization allow data subjects to revoke consent to the processing of their Personal Data (PD)?	3

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Privacy	Product or Service Delivery Restrictions	PRI-03.5	Mechanisms exist to prohibit the refusal of products and/or services on the grounds that a data subject does not agree to the processing of Personal Data (PD) or withdraws consent.	- Privacy Program		Does the organization prohibit the refusal of products and/or services on the grounds that a data subject does not agree to the processing of Personal Data (PD) or withdraws consent?	7
Privacy	Authorized Agent	PRI-03.6	Mechanisms exist to allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions.			Does the organization allow data subjects to authorize another person or entity, acting on the data subject's behalf, to make Personal Data (PD) processing decisions?	6
Privacy	Active Participation By Data Subjects	PRI-03.7	Mechanisms exist to compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.).			Does the organization compel data subjects to select the level of consent deemed appropriate by the data subject for the relevant business purpose (e.g., opt-in, opt-out, accept all cookies, etc.)?	3
Privacy	Global Privacy Control (GPC)	PRI-03.8	Automated mechanisms exist to provide data subjects with functionality to exercise pre-selected opt-out preferences (e.g., opt-out signal).			Does the organization provide data subjects with functionality to automatically exercise pre-selected opt-out preferences (e.g., opt-out signal)?	5
Privacy	Restrict Collection To Identified Purpose	PRI-04	Mechanisms exist to collect Personal Data (PD) only for the purposes identified in the privacy notice and includes protections against collecting PD from minors without appropriate parental, or legal guardian, consent.		E-PRI-02	Does the organization collect Personal Data (PD) only for the purposes identified in the privacy notice?	7
Privacy	Authority To Collect, Use, Maintain & Share Personal Data (PD)	PRI-04.1	Mechanisms exist to determine and document the legal authority that permits the collection, use, maintenance and sharing of Personal Data (PD), either generally or in support of a specific program or system need.		E-PRI-02	Does the organization determine and document the legal authority that permits the collection, use, maintenance and sharing of Personal Data (PD), either generally or in support of a specific program or system need?	7
Privacy	Primary Sources	PRI-04.2	Mechanisms exist to ensure information is directly collected from the data subject, whenever possible.			Does the organization ensure information is directly collected from the data subject, whenever possible?	7
Privacy	Identifiable Image Collection	PRI-04.3	Mechanisms exist to restrict the collection, processing, storage and sharing of photographic and/or video surveillance image collection that can identify individuals to legitimate business needs.	- Privacy Program		Does the organization restrict the collection, processing, storage and sharing of photographic and/or video surveillance image collection that can identify individuals to legitimate business needs?	7
Privacy	Acquired Personal Data (PD)	PRI-04.4	Mechanisms exist to promptly inform data subjects of the utilization purpose when their Personal Data (PD) is acquired and not received directly from the data subject, except where that utilization purpose was disclosed in advance to the data subject.			Does the organization promptly inform data subjects of the utilization purpose when their Personal Data (PD) is acquired and not received directly from the data subject, except where that utilization purpose was disclosed in advance to the data subject?	6
Privacy	Validate Collected Personal Data	PRI-04.5	Mechanisms exist to ensure that the data subject, or authorized representative, validate Personal Data (PD) during the collection process.			Does the organization request that the data subject, or authorized representative, validate Personal Data (PD) during the collection process?	1
Privacy	Re-Validate Collected Personal Data	PRI-04.6	Mechanisms exist to ensure that the data subject, or authorized representative, re-validate that Personal Data (PD) acquired during the collection process is still accurate.			Does the organization request that the data subject, or authorized representative, re-validate that Personal Data (PD) acquired during the collection process is still accurate?	1
Privacy	Personal Data Retention & Disposal	PRI-05	Mechanisms exist to: • Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; • Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and • Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including		E-AST-11 E-PRI-02	Does the organization: • Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; • Disposes of, destroys, erases, and/or anonymizes the PI, regardless of the method of storage; and	8
Privacy	Internal Use of Personal Data For Testing, Training and Research	PRI-05.1	Mechanisms exist to address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing, training and research.		E-PRI-02	Does the organization address the use of Personal Data (PD) for internal testing, training and research that: • Takes measures to limit or minimize the amount of PD used for internal testing, training and research purposes; and • Authorizes the use of PD when such information is required for internal testing,	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Privacy	Personal Data Accuracy & Integrity	PRI-05.2	Mechanisms exist to confirm the accuracy and relevance of Personal Data (PD) throughout the information lifecycle.			Does the organization confirm the accuracy and relevance of Personal Data (PD) throughout the information lifecycle?	5
Privacy	Data Masking	PRI-05.3	Mechanisms exist to mask sensitive information through data anonymization, pseudonymization, redaction or de-identification.			Does the organization mask sensitive information through data anonymization, pseudonymization, redaction or de-identification?	8
Privacy	Usage Restrictions of Sensitive Personal Data	PRI-05.4	Mechanisms exist to restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in privacy notices.			Does the organization restrict the use of Personal Data (PD) to only the authorized purpose(s) consistent with applicable laws, regulations and in privacy notices?	8
Privacy	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish, maintain and update an inventory that contains a listing of all programs and systems identified as collecting, using, maintaining, or sharing Personal Data (PD).		E-AST-08	Does the organization establish, maintain and update an inventory that contains a listing of all programs and systems identified as collecting, using, maintaining, or sharing Personal Data (PD)?	8
Privacy	Personal Data (PD) Inventory Automation Support	PRI-05.6	Automated mechanisms exist to determine if Personal Data (PD) is maintained in electronic form.			Does the organization use automated mechanisms to determine if Personal Data (PD) is maintained in electronic form?	1
Privacy	Personal Data (PD) Categories	PRI-05.7	Mechanisms exist to define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD).		E-PRI-07	Does the organization define and implement data handling and protection requirements for specific categories of sensitive Personal Data (PD)?	5
Privacy	Data Subject Access	PRI-06	Mechanisms exist to provide individuals the ability to access their Personal Data (PD) maintained in organizational systems of records.		E-PRI-06	Does the organization provide individuals the ability to access their Personal Data (PD) maintained in organizational systems of records?	6
Privacy	Correcting Inaccurate Personal Data	PRI-06.1	Mechanisms exist to establish and implement a process for: • Individuals to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and • Disseminating corrections or amendments of PD to other authorized users of the PD.	- Data Protection Impact Assessment (DPIA)		Does the organization establish and implement a process for: • Individuals to have inaccurate Personal Data (PD) maintained by the organization corrected or amended; and • Disseminating corrections or amendments of PD to other authorized users of the PI?	5
Privacy	Notice of Correction or Processing Change	PRI-06.2	Mechanisms exist to notify affected individuals if their Personal Data (PD) has been corrected or amended.	The organization should, in the case of having general written authorization, inform the customer of any intended changes concerning the addition or replacement of subcontractors to process PD, thereby giving the customer the opportunity to object to such changes.		Does the organization notify affected individuals if their Personal Data (PD) has been corrected or amended?	4
Privacy	Appeal Adverse Decision	PRI-06.3	Mechanisms exist to provide an organization-defined process for individuals to appeal an adverse decision and have incorrect information amended.			Does the organization provide an organization-defined process for individuals to appeal an adverse decision and have incorrect information amended?	4
Privacy	User Feedback Management	PRI-06.4	Mechanisms exist to implement a process for receiving and responding to complaints, concerns or questions from individuals about the organizational privacy practices.			Does the organization implement a process for receiving and responding to complaints, concerns or questions from individuals about the organizational privacy practices?	5
Privacy	Right to Erasure	PRI-06.5	Mechanisms exist to erase personal data of an individual, without delay.			Does the organization erase personal data of an individual, without delay?	5
Privacy	Data Portability	PRI-06.6	Mechanisms exist to export Personal Data (PD) in a structured, commonly used and machine-readable format that allows the data subject to transmit the data to another controller without hindrance.			Does the organization export Personal Data (PD) in a structured, commonly used and machine-readable format that allows the data subject to transmit the data to another controller without hindrance?	3

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Privacy	Personal Data Exportability	PRI-06.7	Mechanisms exist to digitally export Personal Data (PD) in a secure manner upon request by the data subject.			Does the organization digitally export Personal Data (PD) in a secure manner upon request by the data subject?	5
Privacy	Information Sharing With Third Parties	PRI-07	Mechanisms exist to disclose Personal Data (PD) to third-parties only for the purposes identified in the privacy notice and with the implicit or explicit consent of the data subject.	- Veris (incident sharing) (http://veriscommunity.net)	E-PRI-05 E-TPM-01	Does the organization disclose Personal Data (PD) to third-parties only for the purposes identified in the privacy notice and with the implicit or explicit consent of the individual?	9
Privacy	Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include privacy requirements in contracts and other acquisition-related documents that establish privacy roles and responsibilities for contractors and service providers.		E-PRI-05 E-TPM-01	Does the organization include privacy requirements in contracts and other acquisition-related documents that establish privacy roles and responsibilities for contractors and service providers?	10
Privacy	Joint Processing of Personal Data	PRI-07.2	Mechanisms exist to clearly define and communicate the organization's role in processing Personal Data (PD) in the data processing ecosystem.		E-PRI-05 E-TPM-01	Does the organization clearly define and communicate the organization's role in processing Personal Data (PD) in the data processing ecosystem?	5
Privacy	Obligation To Inform Third-Parties	PRI-07.3	Mechanisms exist to inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD).	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization inform applicable third-parties of any modification, deletion or other change that affects shared Personal Data (PD)?	5
Privacy	Reject Unauthorized Disclosure Requests	PRI-07.4	Mechanisms exist to reject unauthorized disclosure requests.	- Authorized Agent		Does the organization reject unauthorized disclosure requests?	5
Privacy	Testing, Training & Monitoring	PRI-08	Mechanisms exist to conduct cybersecurity and privacy testing, training and monitoring activities			Does the organization implement a process for ensuring that organizational plans for conducting cybersecurity and privacy testing, training and monitoring activities associated with organizational systems are developed and performed?	8
Privacy	Personal Data Lineage	PRI-09	Mechanisms exist to utilize a record of processing activities to maintain a record of Personal Data (PD) that is stored, transmitted and/or processed under the organization's responsibility.	The organization should determine and securely maintain the necessary records in support of its obligations for the processing of PD.		Does the organization utilize a System of Records Notices (SORN), or similar record of processing activities, to maintain a record of processing Personal Data (PD) under the organization's responsibility?	5
Privacy	Data Quality Management	PRI-10	Mechanisms exist to issue guidelines ensuring and maximizing the quality, utility, objectivity, integrity, impact determination and de-identification of Personal Data (PD) across the information lifecycle.			Does the organization issue guidelines ensuring and maximizing the quality, utility, objectivity, integrity, impact determination and de-identification of Personal Data (PD) across the information lifecycle?	5
Privacy	Automation	PRI-10.1	Automated mechanisms exist to support the evaluation of data quality across the information lifecycle.			Does the organization use automated mechanisms to support the evaluation of data quality across the information lifecycle?	1
Privacy	Data Analytics Bias	PRI-10.2	Mechanisms exist to evaluate its analytical processes for potential bias.			Does the organization evaluate its analytical processes for potential bias?	5
Privacy	Data Tagging	PRI-11	Mechanisms exist to issue data modeling guidelines to support tagging of sensitive/regulated data.			Does the organization issue data modeling guidelines to support tagging of Personal Data (PD)?	3
Privacy	Updating Personal Data (PD)	PRI-12	Mechanisms exist to develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur.			Does the organization develop processes to identify and record the method under which Personal Data (PD) is updated and the frequency that such updates occur?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Privacy	Data Management Board	PRI-13	Mechanisms exist to establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB.	- Data Management Board (DMB)		Does the organization establish a written charter for a Data Management Board (DMB) and assigned organization-defined roles to the DMB?	3
Privacy	Privacy Records & Reporting	PRI-14	Mechanisms exist to maintain privacy-related records and develop, disseminate and update reports to internal senior management, as well as external oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates.			Does the organization develop, disseminate and update reports to internal senior management, as well as external oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates?	8
Privacy	Accounting of Disclosures	PRI-14.1	Mechanisms exist to develop and maintain an accounting of disclosures of Personal Data (PD) held by the organization and make the accounting of disclosures available to the person named in the record, upon request.		E-PRI-01	Does the organization develop and maintain an accounting of disclosures of Personal Data (PD) held by the organization and make the accounting of disclosures available to the person named in the record, upon request?	8
Privacy	Notification of Disclosure Request To Data Subject	PRI-14.2	Mechanisms exist to notify data subjects of applicable legal requests to disclose Personal Data (PD).			Does the organization notify data subjects of applicable legal requests to disclose Personal Data (PD)?	5
Privacy	Register Database	PRI-15	Mechanisms exist to register databases containing Personal Data (PD) with the appropriate Data Authority, when necessary.		E-PRI-03	Does the organization register databases containing Personal Data (PD) with the appropriate Data Authority, when necessary?	3
Privacy	Potential Human Rights Abuses	PRI-16	Mechanisms exist to constrain the supply of physical and/or digital activity logs to the host government that can directly lead to contravention of the Universal Declaration of Human Rights (UDHR), as well as other applicable statutory, regulatory and/or contractual obligations.	- Board of Directors (Bod) Ethics Committee		Does the organization constrain the supply of physical and/or digital activity logs to the host government that can directly lead to contravention of the Universal Declaration of Human Rights (UDHR), as well as other applicable statutory, regulatory and/or contractual obligations?	10
Privacy	Data Subject Communications	PRI-17	Mechanisms exist to craft disclosures and communications to data subjects such that the material is readily accessible and written in a manner that is concise, unambiguous and understandable by a reasonable person.			Does the organization craft disclosures and communications to data subjects such that the material is readily accessible and written in a manner that is concise, unambiguous and understandable by a reasonable person?	6
Privacy	Conspicuous Link To Privacy Notice	PRI-17.1	Mechanisms exist to include a conspicuous link to the organization's privacy notice on all consumer-facing websites and mobile applications.			Does the organization include a conspicuous link to the organization's privacy notice on all consumer-facing websites and mobile applications?	4
Privacy	Notice of Financial Incentive	PRI-17.2	Mechanisms exist to provide data subjects with a Notice of Financial Incentive that explains the material terms of a financial incentive, price or service difference so the data subject can make an informed decision about whether to participate.			Does the organization provide data subjects with a Notice of Financial Incentive that explains the material terms of a financial incentive, price or service difference so the data subject can make an informed decision about whether to participate?	2
Project & Resource Management	Security Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and privacy-related resource planning controls that define a viable plan for achieving cybersecurity & privacy objectives.		E-PRM-02	Does the organization facilitate the implementation of cybersecurity and privacy-related resource planning controls?	8
Project & Resource Management	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and privacy-specific business plan and set of objectives to achieve that plan.		E-PRM-01	Does the organization establish a strategic cybersecurity and privacy-specific business plan and set of objectives to achieve that plan?	5
Project & Resource Management	Targeted Capability Maturity Levels	PRM-01.2	Mechanisms exist to define and identify targeted capability maturity levels.		E-PRM-04	Does the organization define and identify targeted capability maturity levels?	5
Project & Resource Management	Security & Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the security & privacy programs and document all exceptions to this requirement.		E-PRM-02	Does the organization address all capital planning and investment requests, including the resources needed to implement the security & privacy programs and document all exceptions to this requirement?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Project & Resource Management	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and privacy requirements within business process planning for projects / initiatives.		E-PRM-01 E-PRM-02	Does the organization identify and allocate resources for management, operational, technical and privacy requirements within business process planning for projects / initiatives?	8
Project & Resource Management	Security & Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity and privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.		E-PRM-03	Does the organization assess cybersecurity and privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements?	10
Project & Resource Management	Security & Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	- Secure Development Life Cycle (SDLC)	E-PRM-03	Does the organization identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC)?	9
Project & Resource Management	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity and privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.		E-PRM-03	Does the organization define business processes with consideration for cybersecurity and privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and	7
Project & Resource Management	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)	E-PRM-03	Does the organization ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures?	10
Project & Resource Management	Manage Organizational Knowledge	PRM-08	Mechanisms exist to manage the organizational knowledge of the cybersecurity and privacy staff.			Does the organization manage the organizational knowledge. of the cybersecurity and privacy staff?	5
Risk Management	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of risk management controls.	- Risk Management Program (RMP)	E-RSK-01	Does the organization facilitate the implementation of risk management controls?	10
Risk Management	Risk Framing	RSK-01.1	Mechanisms exist to identify: • Assumptions affecting risk assessments, risk response and risk monitoring; • Constraints affecting risk assessments, risk response and risk monitoring; • The organizational risk tolerance; and • Priorities and trade-offs considered by the organization for managing risk.	- Risk Management Program (RMP)		Does the organization identify: • Assumptions affecting risk assessments, risk response and risk monitoring; • Constraints affecting risk assessments, risk response and risk monitoring; • The organizational risk tolerance; and • Priorities and trade-offs considered by the organization for managing risk?	9
Risk Management	Risk Management Resourcing	RSK-01.2	Mechanisms exist to reduce the magnitude or likelihood of potential impacts by resourcing the capability required to manage technology-related risks.			Does the organization reduce the magnitude or likelihood of potential impacts by resourcing the capability required to manage technology-related risks?	8
Risk Management	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance(s).	- Defined risk tolerance	E-RSK-06	Does the organization define organizational risk tolerance(s)?	9
Risk Management	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold.	- Defined risk threshold	E-RSK-07	Does the organization define organizational risk threshold?	9
Risk Management	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize systems and data in accordance with applicable local, state and Federal laws that: • Document the security categorization results (including supporting rationale) in the security plan for systems; and • Ensure the security categorization decision is reviewed and approved by the asset owner.	- Risk Management Program (RMP)		Does the organization categorize systems and data in accordance with applicable local, state and Federal laws that: • Document the security categorization results (including supporting rationale) in the security plan for systems; and • Ensure the security categorization decision is reviewed and approved by the asset	9
Risk Management	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for systems, applications and/or services to prevent potential disruptions.			Does the organization prioritize the impact level for systems, applications and/or services to provide additional granularity on potential disruptions?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Risk Management	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	- Risk Management Program (RMP)		Does the organization identify and document risks, both internal and external?	9
Risk Management	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	- Risk Management Program (RMP) - Risk assessment - Business Impact Analysis (BIA) - Data Protection Impact Assessment (DPIA)	E-RSK-04	Does the organization conduct an annual assessment of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data?	10
Risk Management	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	- Risk Management Program (RMP) - Risk register - Governance, Risk and Compliance Solution (GRC) tool (SCFConnect, SureCloud,Ostendio, ZenGRC, Archer, RSAM, MetricStream, etc.)	E-RSK-03	Does the organization maintain a risk register that facilitates monitoring and reporting of risks?	10
Risk Management	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	- Risk Management Program (RMP)		Does the organization identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices?	9
Risk Management	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	- Risk Management Program (RMP) - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization remediate risks to an acceptable level?	10
Risk Management	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity and privacy assessments, incidents and audits to ensure proper remediation has been performed.	- Risk Management Program (RMP)		Does the organization respond to findings from cybersecurity and privacy assessments, incidents and audits to ensure proper remediation has been performed?	9
Risk Management	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.			Does the organization identify and implement compensating countermeasures to reduce risk and exposure to threats?	9
Risk Management	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	- Risk Management Program (RMP)		Does the organization routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information?	9
Risk Management	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	- Risk Management Program (RMP) - Data Protection Impact Assessment (DPIA) - Business Impact Analysis (BIA)	E-CHG-01	Does the organization conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks?	8
Risk Management	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	- Risk Management Program (RMP)	E-RSK-02	Does the organization develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans?	10
Risk Management	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	- Risk Management Program (RMP) - Data Protection Impact Assessment (DPIA)	E-RSK-05	Does the organization assess supply chain risks associated with systems, system components and services?	9
Risk Management	AI & Autonomous Technologies Supply Chain Impacts	RSK-09.2	Mechanisms exist to address Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks and benefits arising from the organization's supply chain, including third-party software and data.			Does the organization address Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks and benefits arising from the organization's supply chain, including third-party software and data?	8
Risk Management	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	- Risk Management Program (RMP) - Data Protection Impact Assessment (DPIA) - Privacy Impact Assessment (PIA)	E-PRI-04	Does the organization conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Risk Management	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security & privacy controls, compliance and change management.			Does the organization ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of security & privacy controls, compliance and change management?	9
Risk Management	Risk Culture	RSK-12	Mechanisms exist to ensure teams are committed to a culture that considers and communicates technology-related risk.			Does the organization ensure teams are committed to a culture that considers and communicates technology-related risk?	4
Secure Engineering & Architecture	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and privacy practices in the specification, design, development, implementation and modification of systems and services.		E-TDA-01 E-TDA-02 E-TDA-04 E-TDA-08 E-TDA-09	Does the organization facilitate the implementation of industry-recognized cybersecurity and privacy practices in the specification, design, development, implementation and modification of systems and services?	10
Secure Engineering & Architecture	Centralized Management of Cybersecurity & Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity and privacy controls and related processes.			Does the organization centrally-manage the organization-wide management and implementation of cybersecurity and privacy controls and related processes?	9
Secure Engineering & Architecture	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	- Administrative controls through corporate policies, standards & procedures. - NIST 800-160 - Enterprise architecture committee	E-TDA-04 E-TDA-09	Does the organization develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and privacy principles that addresses risk to organizational operations, assets, individuals, other organizations?	9
Secure Engineering & Architecture	Standardized Terminology	SEA-02.1	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.			Does the organization standardize technology and process terminology to reduce confusion amongst groups and departments?	3
Secure Engineering & Architecture	Outsourcing Non-Essential Functions or Services	SEA-02.2	Mechanisms exist to identify non-essential functions or services that are capable of being outsourced to third-party service providers and align with the organization's enterprise architecture and security standards.			Does the organization identify non-essential functions or services that are capable of being outsourced to third-party service providers and align with the organization's enterprise architecture and security standards?	3
Secure Engineering & Architecture	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.			Does the organization conduct ongoing "technical debt" reviews of hardware and software technologies to remediate outdated and/or unsupported technologies?	9
Secure Engineering & Architecture	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.		E-TDA-04 E-TDA-09	Does the organization 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?	10
Secure Engineering & Architecture	System Partitioning	SEA-03.1	Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments.			Does the organization partition systems so that partitions reside in separate physical domains or environments?	8
Secure Engineering & Architecture	Application Partitioning	SEA-03.2	Mechanisms exist to separate user functionality from system management functionality.	- Separate interface for non-privileged users.		Does the organization separate user functionality (including user interface services) from system management functionality?	8
Secure Engineering & Architecture	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.			Does the organization implement a separate execution domain for each executing process?	7
Secure Engineering & Architecture	Security Function Isolation	SEA-04.1	Mechanisms exist to isolate security functions from non-security functions.			Does the organization isolate security functions from non-security functions?	7

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Secure Engineering & Architecture	Hardware Separation	SEA-04.2	Mechanisms exist to implement underlying hardware separation mechanisms to facilitate process separation.			Does the organization implement underlying hardware separation mechanisms to facilitate process separation?	7
Secure Engineering & Architecture	Thread Separation	SEA-04.3	Mechanisms exist to maintain a separate execution domain for each thread in multi-threaded processing.			Does the organization maintain a separate execution domain for each thread in multi-threaded processing?	7
Secure Engineering & Architecture	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.			Does the organization prevent unauthorized and unintended information transfer via shared system resources?	8
Secure Engineering & Architecture	Prevent Program Execution	SEA-06	Automated mechanisms exist to prevent the execution of unauthorized software programs.			Does the organization use automated mechanisms to prevent the execution of unauthorized software programs?	8
Secure Engineering & Architecture	Predictable Failure Analysis	SEA-07	Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.	- Mean Time to Failure (MTTF)		Does the organization determine the Mean Time to Failure (MTTF) for system components in specific environments of operation?	5
Secure Engineering & Architecture	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of systems.	- Computer Lifecycle Program (CLP) - Technology Asset Management (TAM)	E-AST-09	Does the organization manage the usable lifecycles of systems?	7
Secure Engineering & Architecture	Fail Secure	SEA-07.2	Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure.			Does the organization enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure?	8
Secure Engineering & Architecture	Fail Safe	SEA-07.3	Mechanisms exist to implement fail-safe procedures when failure conditions occur.			Does the organization implement fail-safe procedures when failure conditions occur?	8
Secure Engineering & Architecture	Non-Persistence	SEA-08	Mechanisms exist to implement non-persistent system components and services that are initiated in a known state and terminated upon the end of the session of use or periodically at an organization-defined frequency.			Does the organization implement non-persistent system components and services that are initiated in a known state and terminated upon the end of the session of use or periodically at an organization-defined frequency?	9
Secure Engineering & Architecture	Refresh from Trusted Sources	SEA-08.1	Mechanisms exist to ensure that software and data needed for information system component and service refreshes are obtained from trusted sources.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization ensure that software and data needed for information system component and service refreshes are obtained from trusted sources?	5
Secure Engineering & Architecture	Information Output Filtering	SEA-09	Mechanisms exist to validate information output from software programs and/or applications to ensure that the information is consistent with the expected content.			Does the organization validate information output from software programs and/or applications to ensure that the information is consistent with the expected content?	8
Secure Engineering & Architecture	Limit Personal Data (PD) Dissemination	SEA-09.1	Mechanisms exist to limit the dissemination of Personal Data (PD) to organization-defined elements identified in the Data Protection Impact Assessment (DPIA) and consistent with authorized purposes.	- Data Protection Impact Assessment (DPIA)		Does the organization limit the dissemination of Personal Data (PD) to organization-defined elements identified in the Data Protection Impact Assessment (DPIA) and consistent with authorized purposes?	8
Secure Engineering & Architecture	Memory Protection	SEA-10	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	- Puppet (https://puppet.com/) - Chef (https://www.chef.io/) (https://www.chef.io/)		Does the organization implement security safeguards to protect system memory from unauthorized code execution?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Secure Engineering & Architecture	Honeypots	SEA-11	Mechanisms exist to utilize honeypots that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting and analyzing such attacks.			Does the organization utilize honeypots that are specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting and analyzing such attacks?	3
Secure Engineering & Architecture	Honeyclients	SEA-12	Mechanisms exist to utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code.			Does the organization utilize honeyclients that proactively seek to identify malicious websites and/or web-based malicious code?	3
Secure Engineering & Architecture	Heterogeneity	SEA-13	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer (OEM).			Does the organization utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer (OEM)?	3
Secure Engineering & Architecture	Virtualization Techniques	SEA-13.1	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.			Does the organization utilize virtualization techniques to support the employment of a diversity of operating systems and applications?	6
Secure Engineering & Architecture	Concealment & Misdirection	SEA-14	Mechanisms exist to utilize concealment and misdirection techniques for systems to confuse and mislead adversaries.			Does the organization utilize concealment and misdirection techniques for systems to confuse and mislead adversaries?	2
Secure Engineering & Architecture	Randomness	SEA-14.1	Automated mechanisms exist to introduce randomness into organizational operations and assets.			Does the organization introduce randomness into organizational operations and assets?	5
Secure Engineering & Architecture	Change Processing & Storage Locations	SEA-14.2	Automated mechanisms exist to change the location of processing and/or storage at random time intervals.			Does the organization change the location of processing and/or storage at random time intervals?	5
Secure Engineering & Architecture	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.			Does the organization distribute processing and storage across multiple physical locations?	4
Secure Engineering & Architecture	Non-Modifiable Executable Programs	SEA-16	Mechanisms exist to utilize non-modifiable executable programs that load and execute the operating environment and applications from hardware-enforced, read-only media.			Does the organization utilize non-modifiable executable programs that load and execute the operating environment and applications from hardware-enforced, read-only media?	1
Secure Engineering & Architecture	Secure Log-On Procedures	SEA-17	Mechanisms exist to utilize a trusted communications path between the user and the security functions of the system.	- Active Directory (AD) Ctrl+Alt+Del login process		Does the organization utilize a trusted communications path between the user and the security functions of the system?	8
Secure Engineering & Architecture	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to the system that provides privacy and security notices.	- Logon banner - System use notifications - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker		Does the organization utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to the system that provides privacy and security notices?	9
Secure Engineering & Architecture	Standardized Microsoft Windows Banner	SEA-18.1	Mechanisms exist to configure Microsoft Windows-based systems to display an approved logon banner before granting access to the system that provides privacy and security notices.	- Active Directory (AD) Ctrl+Alt+Del login process - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization utilize displays a system use notification / logon banner for Active Directory (AD) users on Microsoft Windows devices before granting access to the system that provides privacy and security notices?	9
Secure Engineering & Architecture	Truncated Banner	SEA-18.2	Mechanisms exist to utilize a truncated system use notification / logon banner on systems not capable of displaying a logon banner from a centralized source, such as Active Directory.	- Logon banner - System use notifications - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker		Does the organization utilize a truncated system use notification / logon banner on systems not capable of displaying a logon banner from a centralized source, such as Active Directory?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Secure Engineering & Architecture	Previous Logon Notification	SEA-19	Mechanisms exist to configure systems that process, store or transmit sensitive/regulated data to notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.	- Network Time Protocol (NTP)		Does the organization configure systems that process, store or transmit sensitive/regulated data to notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon?	3
Secure Engineering & Architecture	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	- Network Time Protocol (NTP)		Does the organization utilize time-synchronization technology to synchronize all critical system clocks?	9
Security Operations	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	- Standardized Operating Procedures (SOP) - ITIL v4 - COBIT 2019		Does the organization facilitate the implementation of operational security controls?	8
Security Operations	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	- Standardized Operating Procedures (SOP)	E-GOV-11	Does the organization use Standardized Operating Procedures (SOP), or similar mechanisms, to identify and document day-to-day procedures to enable the proper execution of assigned tasks?	9
Security Operations	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.			Does the organization develop a security Concept of Operations (CONOPS) that documents management, operational and technical measures implemented to apply defense-in-depth techniques?	9
Security Operations	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	- ITIL v4 - COBIT 2019	E-TPM-04	Does the organization define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards?	7
Security Operations	Security Operations Center (SOC)	OPS-04	Mechanisms exist to establish and maintain a Security Operations Center (SOC) that facilitates a 24x7 response capability.			Does the organization have an internal or outsourced Security Operations Center (SOC) that facilitates a 24x7 response capability?	8
Security Operations	Secure Practices Guidelines	OPS-05	Mechanisms exist to provide guidelines and recommendations for the secure use of products and/or services to assist in the configuration, installation and use of the product and/or service.			Does the organization provide guidelines and recommendations for the secure use of products and/or services to assist in the configuration, installation and use of the product and/or service?	7
Security Awareness & Training	Security & Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.			Does the organization facilitate the implementation of security workforce development and awareness controls?	8
Security Awareness & Training	Security & Privacy Awareness	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.		E-SAT-02	Does the organization provide all employees and contractors appropriate awareness education and training that is relevant for their job function?	8
Security Awareness & Training	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.		E-SAT-03	Does the organization simulate actual cyber-attacks through practical exercises that are aligned with current threat scenarios?	3
Security Awareness & Training	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.		E-SAT-02	Does the organization include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining?	5
Security Awareness & Training	Role-Based Security & Privacy Training	SAT-03	Mechanisms exist to provide role-based security-related training: • Before authorizing access to the system or performing assigned duties; • When required by system changes; and • Annually thereafter.		E-SAT-05	Does the organization provide role-based security-related training: • Before authorizing access to the system or performing assigned duties; • When required by system changes; and • Annually thereafter?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Security Awareness & Training	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in cybersecurity and privacy training that reinforce training objectives.		E-SAT-03	Does the organization include practical exercises in cybersecurity and privacy training that reinforce training objectives?	3
Security Awareness & Training	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.			Does the organization provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior?	9
Security Awareness & Training	Sensitive Information Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive information is formally trained in data handling requirements.			Does the organization ensure that every user accessing a system processing, storing or transmitting sensitive information is formally trained in data handling requirements?	9
Security Awareness & Training	Vendor Security & Privacy Training	SAT-03.4	Mechanisms exist to incorporate vendor-specific security training in support of new technology initiatives.		E-SAT-04 E-SAT-05	Does the organization incorporate vendor-specific security training in support of new technology initiatives?	7
Security Awareness & Training	Privileged Users	SAT-03.5	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities		E-SAT-05	Does the organization provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	9
Security Awareness & Training	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and privacy awareness training that is specific to the cyber threats that the user might encounter the user's specific day-to-day business operations.		E-SAT-04	Does the organization provide role-based cybersecurity and privacy awareness training that is specific to the cyber threats that the user might encounter the user's specific day-to-day business operations?	8
Security Awareness & Training	Continuing Professional Education (CPE) - Cybersecurity & Privacy Personnel	SAT-03.7	Mechanisms exist to ensure cybersecurity and privacy personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry-recognized secure practices that are pertinent to their assigned roles and responsibilities.		E-SAT-01 E-SAT-04	Does the organization ensure cybersecurity and privacy personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry-recognized secure practices that are pertinent to their assigned roles and responsibilities?	8
Security Awareness & Training	Continuing Professional Education (CPE) - DevOps Personnel	SAT-03.8	Mechanisms exist to ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure Software Development Practices (SSDP) to appropriately address evolving threats.			Does the organization ensure application development and operations (DevOps) personnel receive Continuing Professional Education (CPE) training on Secure Software Development Practices (SSDP) to appropriately address evolving threats?	8
Security Awareness & Training	Security & Privacy Training Records	SAT-04	Mechanisms exist to document, retain and monitor individual training activities, including basic security awareness training, ongoing awareness training and specific-system training.	- KnowB4 (https://www.knowbe4.com/)	E-SAT-02 E-SAT-03 E-SAT-04 E-SAT-05	Does the organization document, retain and monitor individual training activities, including basic security awareness training, ongoing awareness training and specific-system training?	9
Technology Development & Acquisition	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.		E-TDA-01 E-TDA-02 E-TDA-08	Does the organization facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs?	10
Technology Development & Acquisition	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies.		E-CPL-06 E-TDA-05 E-TDA-06 E-TDA-07 E-TDA-15	Does the organization design and implement product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies?	10
Technology Development & Acquisition	Integrity Mechanisms for Software / Firmware Updates	TDA-01.2	Mechanisms exist to utilize integrity validation mechanisms for security updates.	- Checksum comparison - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)	E-TDA-15	Does the organization utilize integrity validation mechanisms for security updates?	5
Technology Development & Acquisition	Malware Testing Prior to Release	TDA-01.3	Mechanisms exist to utilize at least one (1) malware detection tool to identify if any known malware exists in the final binaries of the product or security update.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization utilize at least one (1) malware detection tool to identify if any known malware exists in the final binaries of the product or security update?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Technology Development & Acquisition	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to ensure risk-based technical and functional specifications are established to define a Minimum Viable Product (MVP).		E-TDA-06	Does the organization ensure risk-based technical and functional specifications are established to define a Minimum Viable Product (MVP)?	9
Technology Development & Acquisition	Ports, Protocols & Services In Use	TDA-02.1	Mechanisms exist to require the developers of systems, system components or services to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use.	- Ports, Protocols & Services (PPS)	E-CPL-06 E-TDA-07	Does the organization require the developers of systems, system components or services to identify early in the Secure Development Life Cycle (SDLC), the functions, ports, protocols and services intended for use?	8
Technology Development & Acquisition	Information Assurance Enabled Products	TDA-02.2	Mechanisms exist to limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved.	- FIPS 201		Does the organization limit the use of commercially-provided Information Assurance (IA) and IA-enabled IT products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile or the cryptographic module is FIPS-validated or NSA-approved?	2
Technology Development & Acquisition	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software vendors / manufacturers to demonstrate that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed or malformed software.		E-TDA-04	Does the organization require software vendors/manufacturers to demonstrate that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed or malformed software?	5
Technology Development & Acquisition	Pre-Established Security Configurations	TDA-02.4	Mechanisms exist to ensure software vendors / manufacturers: • Deliver the system, component, or service with pre-established security configurations implemented; and • Use the pre-established security configurations as the default for any subsequent system, component, or service reinstallation or upgrade.			Does the organization ensure software vendors / manufacturers: • Deliver the system, component, or service with pre-established security configurations implemented; and • Use the pre-established security configurations as the default for any subsequent system, component, or service reinstallation or upgrade?	8
Technology Development & Acquisition	Identification & Justification of Ports, Protocols & Services	TDA-02.5	Mechanisms exist to require process owners to identify, document and justify the business need for the ports, protocols and other services necessary to operate their technology solutions.		E-CPL-06 E-TDA-07	Does the organization require process owners to identify, document and justify the business need for the ports, protocols and other services necessary to operate their technology solutions?	8
Technology Development & Acquisition	Insecure Ports, Protocols & Services	TDA-02.6	Mechanisms exist to mitigate the risk associated with the use of insecure ports, protocols and services necessary to operate technology solutions.			Does the organization mitigate the risk associated with the use of insecure ports, protocols and services necessary to operate technology solutions?	9
Technology Development & Acquisition	Security & Privacy Representatives For Product Changes	TDA-02.7	Mechanisms exist to include appropriate cybersecurity and privacy representatives in the product feature and/or functionality change control review process.			Does the organization include appropriate cybersecurity and privacy representatives in the product feature and/or functionality change control review process?	10
Technology Development & Acquisition	Commercial Off-The-Shelf (COTS) Security Solutions	TDA-03	Mechanisms exist to utilize only Commercial Off-the-Shelf (COTS) security products.			Does the organization utilize only Commercial Off-the-Shelf (COTS) security products?	5
Technology Development & Acquisition	Supplier Diversity	TDA-03.1	Mechanisms exist to obtain cybersecurity and privacy technologies from different suppliers to minimize supply chain risk.	- Supplier diversity		Does the organization obtain cybersecurity and privacy technologies from different suppliers to minimize supply chain risk?	3
Technology Development & Acquisition	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for systems that describe: • Secure configuration, installation and operation of the system; • Effective use and maintenance of security features/functions; and • Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.		E-CPL-06 E-TDA-06 E-TDA-10	Does the organization obtain, protect and distribute administrator documentation for systems that describe: • Secure configuration, installation and operation of the system; • Effective use and maintenance of security features/functions; and • Known vulnerabilities regarding configuration and use of administrative (e.g.,	8
Technology Development & Acquisition	Functional Properties	TDA-04.1	Mechanisms exist to require vendors/contractors to provide information describing the functional properties of the security controls to be utilized within systems, system components or services in sufficient detail to permit analysis and testing of the controls.	- SSAE-16 SOC2 report	E-CPL-06 E-TDA-06 E-TDA-10 E-TDA-15	Does the organization require vendors/contractors to provide information describing the functional properties of the security controls to be utilized within systems, system components or services in sufficient detail to permit analysis and testing of the controls?	8
Technology Development & Acquisition	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to require a Software Bill of Materials (SBOM) for systems, applications and services that lists software packages in use, including versions and applicable licenses.		E-TDA-12	Does the organization require a Software Bill of Materials (SBOM) for systems, applications and services that lists software packages in use, including versions and applicable licenses?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Technology Development & Acquisition	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of systems, system components or services to produce a design specification and security architecture that: • Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; • Accurately and completely describes the required security functionality and the allocation of security		E-TDA-04	Does the organization require the developers of systems, system components or services to produce a design specification and security architecture that: • Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture;	8
Technology Development & Acquisition	Physical Diagnostic & Test Interfaces	TDA-05.1	Mechanisms exist to secure physical diagnostic and test interfaces to prevent misuse.			Does the organization secure physical diagnostic and test interfaces to prevent misuse?	5
Technology Development & Acquisition	Diagnostic & Test Interface Monitoring	TDA-05.2	Mechanisms exist to enable endpoint devices to log events and generate alerts for attempts to access diagnostic and test interfaces.			Does the organization enable endpoint devices to log events and generate alerts for attempts to access diagnostic and test interfaces?	3
Technology Development & Acquisition	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	- OWASP's Application Security Verification Standard (ASVS) - Mobile Application Security Verification Standard (MASVS)	E-TDA-08 E-TDA-11	Does the organization develop applications based on secure coding principles?	10
Technology Development & Acquisition	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	- Secure Development Life Cycle (SDLC)		Does the organization require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC)?	9
Technology Development & Acquisition	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.		E-TDA-03 E-TDA-10 E-THR-05	Does the organization perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for?	7
Technology Development & Acquisition	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of systems, applications and services.		E-TDA-04 E-TDA-11	Does the organization utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of systems, applications and services?	9
Technology Development & Acquisition	Supporting Toolchain	TDA-06.4	Automated mechanisms exist to improve the accuracy, consistency and comprehensiveness of secure practices throughout the asset's lifecycle.			Does the organization utilize automation to improve the accuracy, consistency and comprehensiveness of secure practices throughout the asset's lifecycle?	6
Technology Development & Acquisition	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to confirm that all cybersecurity and privacy requirements are met and that any identified risks are satisfactorily addressed.		E-TDA-05	Does the organization have an independent review of the software design to confirm that all cybersecurity and privacy requirements are met and that any identified risks are satisfactorily addressed?	10
Technology Development & Acquisition	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.			Does the organization maintain a segmented development network to ensure a secure development environment?	9
Technology Development & Acquisition	Separation of Development, Testing and Operational Environments	TDA-08	Mechanisms exist to manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems.			Does the organization manage separate development, testing and operational environments to reduce the risks of unauthorized access or changes to the operational environment and to ensure no impact to production systems?	10
Technology Development & Acquisition	Secure Migration Practices	TDA-08.1	Mechanisms exist to ensure secure migration practices purge systems, applications and services of test/development/staging data and accounts before it is migrated into a production environment.			Does the organization ensure secure migration practices purge systems, applications and services of test/development/staging data and accounts before it is migrated into a production environment?	8
Technology Development & Acquisition	Security & Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and privacy personnel to: • Create and implement a Security Test and Evaluation (ST&E) plan; • Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and	- Security Test & Evaluation (ST&E)	E-TDA-03 E-TDA-05	Does the organization require system developers/integrators consult with cybersecurity and privacy personnel to: • Create and implement a Security Test and Evaluation (ST&E) plan; • Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Technology Development & Acquisition	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of systems, system components or services to produce a plan for the continuous monitoring of security & privacy control effectiveness.		E-TDA-03	Does the organization require the developers systems, system components or services to produce a plan for the continuous monitoring of security & privacy control effectiveness?	9
Technology Development & Acquisition	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of systems, system components or services to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.		E-TDA-03	Does the organization require the developers of systems, system components or services to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis?	9
Technology Development & Acquisition	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of systems, system components or services to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.		E-TDA-03	Does the organization require the developers of systems, system components or services to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis?	9
Technology Development & Acquisition	Malformed Input Testing	TDA-09.4	Mechanisms exist to utilize testing methods to ensure systems, services and products continue to operate as intended when subject to invalid or unexpected inputs on its interfaces.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)	E-TDA-03	Does the organization utilize testing methods to ensure systems, services and products continue to operate as intended when subject to invalid or unexpected inputs on its interfaces?	7
Technology Development & Acquisition	Application Penetration Testing	TDA-09.5	Mechanisms exist to perform application-level penetration testing of custom-made applications and services.	- NNT Change Tracker (https://www.newnettechnologies.com)	E-TDA-03	Does the organization perform application-level penetration testing of custom-made applications and services?	9
Technology Development & Acquisition	Secure Settings By Default	TDA-09.6	Mechanisms exist to implement secure configuration settings by default to reduce the likelihood of software being deployed with weak security settings that would put the asset at a greater risk of compromise.		E-TDA-03	Does the organization implement secure configuration settings by default to reduce the likelihood of software being deployed with weak security settings that would put the asset at a greater risk of compromise?	9
Technology Development & Acquisition	Manual Code Review	TDA-09.7	Mechanisms exist to require the developers of systems, system components or services to employ a manual code review process to identify and remediate unique flaws that require knowledge of the application's requirements and design.			Does the organization require the developers of systems, system components or services to employ a manual code review process to identify and remediate unique flaws that require knowledge of the application's requirements and design?	5
Technology Development & Acquisition	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.			Does the organization approve, document and control the use of live data in development and test environments?	9
Technology Development & Acquisition	Test Data Integrity	TDA-10.1	Mechanisms exist to ensure the integrity of test data through existing security & privacy controls.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization ensure the integrity of test data through existing security & privacy controls?	8
Technology Development & Acquisition	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.			Does the organization govern component authenticity by developing and implementing anti-counterfeit procedures that include the means to detect and prevent counterfeit components?	9
Technology Development & Acquisition	Anti-Counterfeit Training	TDA-11.1	Mechanisms exist to train personnel to detect counterfeit system components, including hardware, software and firmware.			Does the organization train personnel to detect counterfeit system components, including hardware, software and firmware?	6
Technology Development & Acquisition	~~Component Disposal~~	~~TDA-11.2~~	[deprecated - incorporated into AST-09] ~~Mechanisms exist to dispose of system components using organization-defined techniques and methods to prevent such components from entering the gray market.~~			[deprecated - incorporated into AST-09]	9
Technology Development & Acquisition	Customized Development of Critical Components	TDA-12	Mechanisms exist to custom-develop critical system components, when COTS solutions are unavailable.	- OWASP		Does the organization custom-develop critical system components, when COTS solutions are unavailable?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Technology Development & Acquisition	Developer Screening	TDA-13	Mechanisms exist to ensure that the developers of systems, applications and/or services have the requisite skillset and appropriate access authorizations.			Does the organization ensure that the developers of systems, applications and/or services have the requisite skillset and appropriate access authorizations?	9
Technology Development & Acquisition	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.			Does the organization require system developers and integrators to perform configuration management during system design, development, implementation and operation?	9
Technology Development & Acquisition	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developer of systems, system components or services to enable integrity verification of software and firmware components.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization require developer of systems, system components or services to enable integrity verification of software and firmware components?	8
Technology Development & Acquisition	Hardware Integrity Verification	TDA-14.2	Mechanisms exist to require developer of systems, system components or services to enable integrity verification of hardware components.			Does the organization require developer of systems, system components or services to enable integrity verification of hardware components?	5
Technology Development & Acquisition	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party.	- Security Test and Evaluation (ST&E) plan		Does the organization require system developers and integrators to create a Security Test and Evaluation (ST&E) plan and implement the plan under the witness of an independent party?	9
Technology Development & Acquisition	Developer-Provided Training	TDA-16	Mechanisms exist to require the developers of systems, system components or services to provide training on the correct use and operation of the system, system component or service.			Does the organization require the developers of systems, system components or services to provide training on the correct use and operation of the system, system component or service?	9
Technology Development & Acquisition	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: • Replacing systems when support for the components is no longer available from the developer, vendor or manufacturer; and • Requiring justification and documented approval for the continued use of unsupported system components required to satisfy mission/business needs.		E-AST-09	Does the organization prevent unsupported systems by: • Replacing systems when support for the components is no longer available from the developer, vendor or manufacturer; and • Requiring justification and documented approval for the continued use of unsupported system components required to satisfy mission/business needs?	10
Technology Development & Acquisition	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported system components.			Does the organization provide in-house support or contract external providers for support with unsupported system components?	8
Technology Development & Acquisition	Input Data Validation	TDA-18	Mechanisms exist to check the validity of information inputs.			Does the organization check the validity of information inputs?	9
Technology Development & Acquisition	Error Handling	TDA-19	Mechanisms exist to handle error conditions by: • Identifying potentially security-relevant error conditions; • Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and			Does the organization handle error conditions by: • Identifying potentially security-relevant error conditions; • Generating error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited; and	9
Technology Development & Acquisition	Access to Program Source Code	TDA-20	Mechanisms exist to limit privileges to change software resident within software libraries.	- Source code escrow		Does the organization limit privileges to change software resident within software libraries?	9
Technology Development & Acquisition	Software Release Integrity Verification	TDA-20.1	Mechanisms exist to publish integrity verification information for software releases.			Does the organization publish integrity verification information for software releases?	6
Technology Development & Acquisition	Archiving Software Releases	TDA-20.2	Mechanisms exist to archive software releases and all of their components (e.g., code, package files, third-party libraries, documentation) to maintain integrity verification information.			Does the organization archive software releases and all of their components (e.g., code, package files, third-party libraries, documentation) to maintain integrity verification information?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Technology Development & Acquisition	Software Escrow	TDA-20.3	Mechanisms exist to escrow source code and supporting documentation to ensure software availability in the event the software provider goes out of business or is unable to provide support.		E-TDA-13	Does the organization escrow source code and supporting documentation to ensure software availability in the event the software provider goes out of business or is unable to provide support?	7
Third-Party Management	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	- Procurement program - Contract reviews	E-TPM-03	Does the organization facilitate the implementation of third-party management controls?	10
Third-Party Management	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of Third-Party Service Providers (TSP) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.		E-AST-06 E-DCH-06	Does the organization maintain a current, accurate and complete list of Third-Party Service Providers (TSP) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data?	8
Third-Party Management	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.	- Data Protection Impact Assessment (DPIA)	E-TPM-02	Does the organization identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process?	9
Third-Party Management	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	- Data Protection Impact Assessment (DPIA)	E-RSK-02	Does the organization evaluate security risks associated with the services and product supply chain?	9
Third-Party Management	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.	- Data Protection Impact Assessment (DPIA)		Does the organization utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services?	9
Third-Party Management	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.	- Data Protection Impact Assessment (DPIA) - Liability clause in contracts		Does the organization utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain?	9
Third-Party Management	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	- Data Protection Impact Assessment (DPIA)		Does the organization address identified weaknesses or deficiencies in the security of the supply chain	9
Third-Party Management	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	- Conduct an organizational assessment of risk prior to the acquisition or outsourcing of services. - Maintain and implement policies and procedures to manage service providers (e.g., Software-as-a-Service (SaaS), web hosting companies, collocation providers, or	E-CPL-06	Does the organization mitigate the risks associated with third-party access to the organization's systems and data?	10
Third-Party Management	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	- Conduct an organizational assessment of risk prior to the acquisition or outsourcing of services. - Maintain a list of service providers. - Maintain and implement controls to manage security providers (e.g., backup tape storage facilities or security		Does the organization conduct a risk assessment prior to the acquisition or outsourcing of technology-related services?	9
Third-Party Management	External Connectivity Requirements - Identification of Ports, Protocols & Services	TPM-04.2	Mechanisms exist to require Third-Party Service Providers (TSP) to identify and document the business need for ports, protocols and other services it requires to operate its processes and technologies.		E-CPL-06 E-TDA-07	Does the organization require process owners to identify the ports, protocols and other services required for the use of such services?	7
Third-Party Management	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of third-party service providers are consistent with and reflect organizational interests.	- Third-party contract requirements for cybersecurity controls		Does the organization ensure that the interests of third-party service providers are consistent with and reflect organizational interests?	8
Third-Party Management	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.		E-AST-23	Does the organization restrict the location of information processing/storage based on business requirements?	10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Third-Party Management	Third-Party Contract Requirements	TPM-05	Mechanisms exist to identify, regularly review and document third-party confidentiality, Non-Disclosure Agreements (NDAs) and other contracts that reflect the organization's needs to protect systems and data.	- Non-Disclosure Agreements (NDAs)	E-TPM-01 E-TPM-03	Does the organization identify, regularly review and document third-party confidentiality, Non-Disclosure Agreements (NDAs) and other contracts that reflect the organization's needs to protect systems and data?	10
Third-Party Management	Security Compromise Notification Agreements	TPM-05.1	Mechanisms exist to compel Third-Party Service Providers (TSP) 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.			Does the organization compel Third-Party Service Providers (TSP) 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?	9
Third-Party Management	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.			Does the organization ensure cybersecurity and privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers?	9
Third-Party Management	Third-Party Authentication Practices	TPM-05.3	Mechanisms exist to ensure Third-Party Service Providers (TSP) use unique authentication factors for each of its customers.			Does the organization ensure Third-Party Service Providers (TSP) use unique authentication factors for each of its customers?	8
Third-Party Management	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and privacy controls between internal stakeholders and Third-Party Service Providers (TSP).	- Customer Responsibility Matrix (CRM) - Shared Responsibility Matrix (SRM) - Responsible, Accountable, Supporting, Consulted and Informed (RASCI) matrix	E-CPL-03	Does the organization formally document a Customer Responsibility Matrix (CRM), delineating assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers.?	8
Third-Party Management	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.		E-TPM-03	Does the organization perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders?	10
Third-Party Management	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable Third-Party Service Providers (TSP) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and privacy controls, including any flow-down requirements to subcontractors.			Does the organization obtain a First-Party Declaration (1PD) from applicable Third-Party Service Providers (TSP) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and privacy controls, including any flow-down requirements to subcontractors?	7
Third-Party Management	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or privacy controls.		E-TPM-05	Does the organization include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or privacy controls?	9
Third-Party Management	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.			Does the organization control personnel security requirements including security roles and responsibilities for third-party providers?	9
Third-Party Management	Monitoring for Third-Party Information Disclosure	TPM-07	Mechanisms exist to monitor for evidence of unauthorized exfiltration or disclosure of organizational information.			Does the organization monitor for evidence of unauthorized exfiltration or disclosure of organizational information?	8
Third-Party Management	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit Third-Party Service Providers (TSP) for compliance with established contractual requirements for cybersecurity and privacy controls.		E-TPM-03	Does the organization monitor, regularly review and audit Third-Party Service Providers (TSP) for compliance with established contractual requirements for cybersecurity and privacy controls?	9
Third-Party Management	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.		E-TPM-03	Does the organization address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements?	9
Third-Party Management	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.	- Contact requirement to report changes to service offerings that may impact the contract. - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization 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?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Third-Party Management	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.			Does the organization ensure response/recovery planning and testing are conducted with critical suppliers/providers?	8
Threat Management	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.		E-THR-04	Does the organization implement a threat awareness program that includes a cross-organization information-sharing capability?	8
Threat Management	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.	- Indicators of Exposure (IoE)	E-THR-01	Does the organization develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization?	8
Threat Management	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	- US-CERT mailing lists & feeds - InfraGard - Internal newsletters	E-THR-03	Does the organization maintain situational awareness of evolving threats?	8
Threat Management	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	- Insider threat program	E-THR-04	Does the organization implement an insider threat program that includes a cross-discipline insider threat incident handling team?	8
Threat Management	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.			Does the organization utilize security awareness training on recognizing and reporting potential indicators of insider threat?	8
Threat Management	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.	- "bug bounty" program	E-TDA-16	Does the organization 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?	8
Threat Management	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.		E-THR-05	Does the organization perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls?	4
Threat Management	Tainting	THR-08	Mechanisms exist to embed false data or steganographic data in files to enable the organization to determine if data has been exfiltrated and provide a means to identify the individual(s) involved.			Does the organization embed false data or steganographic data in files to enable the organization to determine if data has been exfiltrated and provide a means to identify the individual(s) involved?	1
Vulnerability & Patch Management	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	- Vulnerability & Patch Management Program (ComplianceForge)	E-MNT-03 E-THR-05 E-VPM-01	Does the organization facilitate the implementation and monitoring of vulnerability management controls?	9
Vulnerability & Patch Management	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.			Does the organization define and manage the scope for its attack surface management activities?	5
Vulnerability & Patch Management	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization ensure that vulnerabilities are properly identified, tracked and remediated?	10
Vulnerability & Patch Management	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	- US-CERT		Does the organization identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Vulnerability & Patch Management	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.	- NNT Change Tracker (https://www.newnettechnologies.com)	E-MNT-03 E-THR-05	Does the organization address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks?	8
Vulnerability & Patch Management	Stable Versions	VPM-04.1	Mechanisms exist to install the latest stable version of any software and/or security-related updates on all applicable systems.			Does the organization install the latest stable version of any security-related updates on all applicable systems?	8
Vulnerability & Patch Management	Flaw Remediation with Personal Data (PD)	VPM-04.2	Mechanisms exist to identify and correct flaws related to the collection, usage, processing or dissemination of Personal Data (PD).			Does the organization identify and correct flaws related to the collection, usage, processing or dissemination of Personal Data (PD)?	8
Vulnerability & Patch Management	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	- Patch management tools	E-MNT-03	Does the organization conduct software patching for all deployed operating systems, applications and firmware?	10
Vulnerability & Patch Management	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	- Patch management tools		Does the organization centrally-manage the flaw remediation process?	9
Vulnerability & Patch Management	Automated Remediation Status	VPM-05.2	Automated mechanisms exist to determine the state of system components with regard to flaw remediation.	- Vulnerability scanning tools - CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization use automated mechanisms to determine the state of system components with regard to flaw remediation?	9
Vulnerability & Patch Management	Time To Remediate / Benchmarks For Corrective Action	VPM-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization track the effectiveness of remediation operations through metrics reporting?	6
Vulnerability & Patch Management	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.			Does the organization install the latest stable versions of security-relevant software and firmware updates?	5
Vulnerability & Patch Management	Removal of Previous Versions	VPM-05.5	Mechanisms exist to remove old versions of software and firmware components after updated versions have been installed.			Does the organization remove old versions of software and firmware components after updated versions have been installed?	5
Vulnerability & Patch Management	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by recurring vulnerability scanning of systems and web applications.	- External vulnerability scans (unauthenticated) - Internal vulnerability scans (authenticated) - Nessus (https://www.tenable.com/products/nessus/nessus-professional) - Qualys (https://www.qualys.com/)	E-VPM-05	Does the organization detect vulnerabilities and configuration errors by recurring vulnerability scanning of systems and web applications?	9
Vulnerability & Patch Management	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.			Does the organization update vulnerability scanning tools?	8
Vulnerability & Patch Management	Breadth / Depth of Coverage	VPM-06.2	Mechanisms exist to identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - NNT Change Tracker (https://www.newnettechnologies.com)		Does the organization identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for?	8
Vulnerability & Patch Management	Privileged Access	VPM-06.3	Mechanisms exist to implement privileged access authorization for selected vulnerability scanning activities.	- Authenticated scans		Does the organization implement privileged access authorization for selected vulnerability scanning activities?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Vulnerability & Patch Management	Trend Analysis	VPM-06.4	Automated mechanisms exist to compare the results of vulnerability scans over time to determine trends in system vulnerabilities.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/)		Does the organization use automated mechanisms to compare the results of vulnerability scans over time to determine trends in system vulnerabilities?	9
Vulnerability & Patch Management	Review Historical Audit Logs	VPM-06.5	Mechanisms exist to review historical audit logs to determine if identified vulnerabilities have been previously exploited.			Does the organization review historical audit logs to determine if identified vulnerabilities have been previously exploited?	9
Vulnerability & Patch Management	External Vulnerability Assessment Scans	VPM-06.6	Mechanisms exist to perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).		E-VPM-05	Does the organization perform quarterly external vulnerability scans (outside the organization's network looking inward) via a reputable vulnerability service provider, which include rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS)?	9
Vulnerability & Patch Management	Internal Vulnerability Assessment Scans	VPM-06.7	Mechanisms exist to perform quarterly internal vulnerability scans, which includes all segments of the organization's internal network, as well as rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS).		E-VPM-05	Does the organization perform quarterly internal vulnerability scans, which includes all segments of the organization's internal network, as well as rescans until passing results are obtained or all "high" vulnerabilities are resolved, as defined by the Common Vulnerability Scoring System (CVSS)?	9
Vulnerability & Patch Management	Acceptable Discoverable Information	VPM-06.8	Mechanisms exist to define what information is allowed to be discoverable by adversaries and take corrective actions to remediated non-compliant systems.			Does the organization define what information is allowed to be discoverable by adversaries and take corrective actions to remediated non-compliant systems?	5
Vulnerability & Patch Management	Correlate Scanning Information	VPM-06.9	Automated mechanisms exist to correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors.			Does the organization correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability/multi-hop attack vectors?	5
Vulnerability & Patch Management	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.		E-VPM-02 E-VPM-03	Does the organization conduct penetration testing on systems and web applications?	9
Vulnerability & Patch Management	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.		E-VPM-04	Does the organization utilize an independent assessor or penetration team to perform penetration testing?	6
Vulnerability & Patch Management	Technical Surveillance Countermeasures Security	VPM-08	Mechanisms exist to utilize a technical surveillance countermeasures survey.	- Facility sweeping for "bugs" or other unauthorized surveillance technologies.		Does the organization utilize a technical surveillance countermeasures survey?	1
Vulnerability & Patch Management	Reviewing Vulnerability Scanner Usage	VPM-09	Mechanisms exist to monitor logs associated with scanning activities and associated administrator accounts to ensure that those activities are limited to the timeframes of legitimate scans.	- Security Incident Event Manager (SIEM)		Does the organization monitor logs associated with scanning activities and associated administrator accounts to ensure that those activities are limited to the timeframes of legitimate scans?	3
Vulnerability & Patch Management	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise systems and applications in accordance with organization-defined rules of engagement.	- "red team" exercises		Does the organization utilize "red team" exercises to simulate attempts by adversaries to compromise systems and applications in accordance with organization-defined rules of engagement?	3
Web Security	Web Security	WEB-01	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.			Does the organization facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures?	8
Web Security	Unauthorized Code	WEB-01.1	Mechanisms exist to prevent unauthorized code from being present in a secure page as it is rendered in a client's browser.			Does the organization prevent unauthorized code from being present in a secure page as it is rendered in a client's browser?	9

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Web Security	Use of Demilitarized Zones (DMZ)	WEB-02	Mechanisms exist to utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports.			Does the organization utilize a Demilitarized Zone (DMZ) to restrict inbound traffic to authorized devices on certain services, protocols and ports?	9
Web Security	Web Application Firewall (WAF)	WEB-03	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	- Web Application Firewall (WAF)		Does the organization deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats?	8
Web Security	Client-Facing Web Services	WEB-04	Mechanisms exist to deploy reasonably-expected security controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service.	- OWASP		Does the organization deploy reasonably-expected security controls to protect the confidentiality and availability of client data that is stored, transmitted or processed by the Internet-based service?	10
Web Security	Cookie Management	WEB-05	Mechanisms exist to provide individuals with clear and precise information about cookies, in accordance with applicable legal requirements for cookie management.			Does the organization provide individuals with clear and precise information about cookies, in accordance with regulatory requirements for cookie management?	5
Web Security	Strong Customer Authentication (SCA)	WEB-06	Mechanisms exist to implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.			Does the organization implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity?	8
Web Security	Web Security Standard	WEB-07	Mechanisms exist to ensure the Open Web Application Security Project (OWASP) Application Security Verification Standard is incorporated into the organization's Secure Systems Development Lifecycle (SSDLC) process.			Does the organization ensure the Open Web Application Security Project (OWASP) Application Security Verification Standard is followed when developing web applications?	9
Web Security	Web Application Framework	WEB-08	Mechanisms exist to ensure a robust Web Application Framework is used to aid in the development of secure web applications, including web services, web resources and web APIs.			Does the organization ensure a robust Web Application Framework is used to aid in the development of secure web applications, including web services, web resources and web APIs?	9
Web Security	Validation & Sanitization	WEB-09	Mechanisms exist to ensure all input handled by a web application is validated and/or sanitized.			Does the organization ensure all input handled by a web application is validated and/or sanitized?	9
Web Security	Secure Web Traffic	WEB-10	Mechanisms exist to ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS).			Does the organization ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS)?	9
Web Security	Output Encoding	WEB-11	Mechanisms exist to ensure output encoding is performed on all content produced by a web application to reduce the likelihood of cross-site scripting and other injection attacks.			Does the organization ensure output encoding is performed on all content produced by a web application to reduce the likelihood of cross-site scripting and other injection attacks?	9
Web Security	Web Browser Security	WEB-12	Mechanisms exist to ensure web applications implement Content-Security-Policy, HSTS and X-Frame-Options response headers to protect both the web application and its users.			Does the organization ensure web applications implement Content-Security-Policy, HSTS and X-Frame-Options response headers to protect both the web application and its users?	9
Web Security	Website Change Detection	WEB-13	Mechanisms exist to detect and respond to Indicators of Compromise (IoC) for unauthorized alterations, additions, deletions or changes on websites that store, process and/or transmit sensitive / regulated data.			Does the organization detect and respond to Indicators of Compromise (IoC) for unauthorized alterations, additions, deletions or changes on websites that store, process and/or transmit sensitive / regulated data?	8

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

GOV-01	GOV-01_A06
GOV-01	GOV-01_A07
GOV-01	GOV-01_A08
GOV-01	GOV-01_A09
GOV-01	GOV-01_A10
GOV-01	GOV-01_A11
GOV-01	GOV-01_A12
GOV-01	GOV-01_A13
GOV-01	GOV-01_A14
GOV-01	GOV-01_A15
GOV-01	GOV-01_A16
GOV-01	GOV-01_A17
GOV-01	GOV-01_A18
GOV-01.1	GOV-01.1_A01
GOV-01.1	GOV-01.1_A02
GOV-01.2	GOV-01.2_A01
GOV-02	GOV-02_A01
GOV-02	GOV-02_A02
GOV-02	GOV-02_A03
GOV-02	GOV-02_A04
GOV-02	GOV-02_A05
GOV-02	GOV-02_A06
GOV-02	GOV-02_A07
GOV-02	GOV-02_A08
GOV-02	GOV-02_A09
GOV-02	GOV-02_A10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

GOV-03	GOV-03_A04
GOV-04	GOV-04_A01
GOV-04	GOV-04_A02
GOV-04	GOV-04_A03
GOV-04	GOV-04_A04
GOV-04	GOV-04_A05
GOV-04.1	GOV-04.1_A01
GOV-04.1	GOV-04.1_A02
GOV-04.2	GOV-04.2_A01
GOV-04.2	GOV-04.2_A02
GOV-05	GOV-05_A01
GOV-05	GOV-05_A02
GOV-05	GOV-05_A03
GOV-05	GOV-05_A04
GOV-05	GOV-05_A05
GOV-05	GOV-05_A06
GOV-05.1	GOV-05.1_A01
GOV-05.2	GOV-05.2_A01
GOV-06	GOV-06_A01
GOV-06	GOV-06_A02
GOV-07	GOV-07_A01
GOV-07	GOV-07_A02
GOV-07	GOV-07_A03
GOV-08	GOV-08_A01
GOV-08	GOV-08_A02
GOV-09	GOV-09_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

GOV-11	GOV-11_A01
GOV-11	GOV-11_A02
GOV-12	GOV-12_A01
GOV-12	GOV-12_A02
GOV-12	GOV-12_A03
GOV-13	GOV-13_A01
GOV-13	GOV-13_A02
GOV-13	GOV-13_A03
GOV-14	GOV-14_A01
GOV-14	GOV-14_A02
GOV-14	GOV-14_A03
GOV-15	GOV-15_A01
GOV-15	GOV-15_A02
GOV-15.1	GOV-15.1_A01
GOV-15.1	GOV-15.1_A02
GOV-15.2	GOV-15.2_A01
GOV-15.2	GOV-15.2_A02
GOV-15.3	GOV-15.3_A01
GOV-15.3	GOV-15.3_A02
GOV-15.4	GOV-15.4_A01
GOV-15.4	GOV-15.4_A02
GOV-15.5	GOV-15.5_A01
GOV-15.5	GOV-15.5_A02
AAT-01	AAT-01_A01
AAT-01	AAT-01_A02
AAT-01.1	AAT-01.1_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

AAT-02.1	AAT-02.1_A02
AAT-02.1	AAT-02.1_A03
AAT-02.2	AAT-02.2_A01
AAT-02.2	AAT-02.2_A02
AAT-03	AAT-03_A01
AAT-03	AAT-03_A02
AAT-03	AAT-03_A03
AAT-03	AAT-03_A04
AAT-03	AAT-03_A05
AAT-03.1	AAT-03.1_A01
AAT-03.1	AAT-03.1_A02
AAT-04	AAT-04_A01
AAT-04	AAT-04_A02
AAT-04	AAT-04_A03
AAT-04	AAT-04_A04
AAT-04	AAT-04_A05
AAT-04.1	AAT-04.1_A01
AAT-04.2	AAT-04.2_A01
AAT-04.3	AAT-04.3_A01
AAT-04.4	AAT-04.4_A01
AAT-04.4	AAT-04.4_A02
AAT-04.4	AAT-04.4_A03
AAT-04.4	AAT-04.4_A04
AAT-05	AAT-05_A01
AAT-05	AAT-05_A02
AAT-05	AAT-05_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

AAT-07	AAT-07_A04
AAT-07	AAT-07_A05
AAT-07.1	AAT-07.1_A01
AAT-07.1	AAT-07.1_A02
AAT-07.1	AAT-07.1_A03
AAT-07.1	AAT-07.1_A04
AAT-07.1	AAT-07.1_A05
AAT-07.2	AAT-07.2_A01
AAT-07.2	AAT-07.2_A02
AAT-07.3	AAT-07.3_A01
AAT-08	AAT-08_A01
AAT-08	AAT-08_A02
AAT-08	AAT-08_A03
AAT-08	AAT-08_A04
AAT-08	AAT-08_A05
AAT-09	AAT-09_A01
AAT-09	AAT-09_A02
AAT-10	AAT-10_A01
AAT-10	AAT-10_A02
AAT-10	AAT-10_A03
AAT-10	AAT-10_A04
AAT-10	AAT-10_A05
AAT-10.1	AAT-10.1_A01
AAT-10.2	AAT-10.2_A01
AAT-10.2	AAT-10.2_A02
AAT-10.2	AAT-10.2_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

AAT-10.6	AAT-10.6_A01
AAT-10.6	AAT-10.6_A02
AAT-10.7	AAT-10.7_A01
AAT-10.8	AAT-10.8_A01
AAT-10.9	AAT-10.9_A01
AAT-10.10	AAT-10.10_A01
AAT-10.11	AAT-10.11_A01
AAT-10.12	AAT-10.12_A01
AAT-10.12	AAT-10.12_A02
AAT-10.13	AAT-10.13_A01
AAT-10.14	AAT-10.14_A01
AAT-11	AAT-11_A01
AAT-11	AAT-11_A02
AAT-11.1	AAT-11.1_A01
AAT-11.1	AAT-11.1_A02
AAT-11.2	AAT-11.2_A01
AAT-11.3	AAT-11.3_A01
AAT-11.3	AAT-11.3_A02
AAT-11.4	AAT-11.4_A01
AAT-12	AAT-12_A01
AAT-12	AAT-12_A02
AAT-12	AAT-12_A03
AAT-13	AAT-13_A01
AAT-13	AAT-13_A02
AAT-13	AAT-13_A03
AAT-13.1	AAT-13.1_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

AAT-15	AAT-15_A01
AAT-15	AAT-15_A02
AAT-15.1	AAT-15.1_A01
AAT-15.1	AAT-15.1_A02
AAT-15.2	AAT-15.2_A01
AAT-15.2	AAT-15.2_A02
AAT-16	AAT-16_A01
AAT-16.1	AAT-16.1_A01
AAT-16.1	AAT-16.1_A02
AAT-16.2	AAT-16.2_A01
AAT-16.3	AAT-16.3_A01
AAT-16.3	AAT-16.3_A02
AAT-16.4	AAT-16.4_A01
AAT-16.4	AAT-16.4_A02
AAT-16.5	AAT-16.5_A01
AAT-16.6	AAT-16.6_A01
AAT-16.7	AAT-16.7_A01
AAT-17	AAT-17_A01
AAT-17	AAT-17_A02
AAT-17.1	AAT-17.1_A01
AAT-17.1	AAT-17.1_A02
AAT-17.2	AAT-17.2_A01
AAT-17.2	AAT-17.2_A02
AAT-17.3	AAT-17.3_A01
AAT-18	AAT-18_A01
AAT-18.1	AAT-18.1_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

AST-01.2	AST-01.2_A02
AST-01.3	AST-01.3_A01
AST-02	AST-02_A01
AST-02	AST-02_A02
AST-02	AST-02_A03
AST-02	AST-02_A04
AST-02	AST-02_A05
AST-02	AST-02_A06
AST-02	AST-02_A07
AST-02.1	AST-02.1_A01
AST-02.1	AST-02.1_A02
AST-02.1	AST-02.1_A03
AST-02.2	AST-02.2_A01
AST-02.2	AST-02.2_A02
AST-02.2	AST-02.2_A03
AST-02.2	AST-02.2_A04
AST-02.2	AST-02.2_A05
AST-02.2	AST-02.2_A06
AST-02.2	AST-02.2_A07
AST-02.3	AST-02.3_A01
AST-02.3	AST-02.3_A02
AST-02.3	AST-02.3_A03
AST-02.3	AST-02.3_A04
AST-02.3	AST-02.3_A05
AST-02.4	AST-02.4_A01
AST-02.4	AST-02.4_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

AST-02.6	AST-02.6_A02
AST-02.7	AST-02.7_A01
AST-02.7	AST-02.7_A02
AST-02.8	AST-02.8_A01
AST-02.9	AST-02.9_A01
AST-02.9	AST-02.9_A02
AST-02.9	AST-02.9_A03
AST-02.9	AST-02.9_A04
AST-02.9	AST-02.9_A05
AST-02.10	AST-02.10_A01
AST-02.10	AST-02.10_A02
AST-02.11	AST-02.11_A01
AST-02.11	AST-02.11_A02
AST-02.11	AST-02.11_A03
AST-03	AST-03_A01
AST-03.1	AST-03.1_A01
AST-03.2	AST-03.2_A01
AST-03.2	AST-03.2_A02
AST-03.2	AST-03.2_A03
AST-03.2	AST-03.2_A04
AST-03.2	AST-03.2_A05
AST-03.2	AST-03.2_A06
AST-03.2	AST-03.2_A07
AST-03.2	AST-03.2_A08
AST-03.2	AST-03.2_A09
AST-03.2	AST-03.2_A10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

AST-04	AST-04_A07
AST-04	AST-04_A08
AST-04.1	AST-04.1_A01
AST-04.1	AST-04.1_A02
AST-04.2	AST-04.2_A01
AST-04.3	AST-04.3_A01
AST-04.3	AST-04.3_A02
AST-05	AST-05_A01
AST-05.1	AST-05.1_A01
AST-06	AST-06_A01
AST-06.1	AST-06.1_A01
AST-07	AST-07_A01
AST-08	AST-08_A01
AST-08	AST-08_A02
AST-09	AST-09_A01
AST-09	AST-09_A02
AST-09	AST-09_A03
AST-09	AST-09_A04
AST-09	AST-09_A05
AST-09	AST-09_A06
AST-09	AST-09_A07
AST-10	AST-10_A01
AST-10	AST-10_A02
AST-11	AST-11_A01
AST-11	AST-11_A02
AST-11	AST-11_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

AST-14	AST-14_A04
AST-14	AST-14_A05
AST-14.1	AST-14.1_A01
AST-14.1	AST-14.1_A02
AST-14.2	AST-14.2_A01
AST-14.2	AST-14.2_A02
AST-15	AST-15_A01
AST-15	AST-15_A02
AST-15.1	AST-15.1_A01
AST-15.1	AST-15.1_A02
AST-15.1	AST-15.1_A03
AST-15.1	AST-15.1_A04
AST-16	AST-16_A01
AST-17	AST-17_A01
AST-18	AST-18_A01
AST-18	AST-18_A02
AST-18	AST-18_A03
AST-19	AST-19_A01
AST-20	AST-20_A01
AST-20	AST-20_A02
AST-21	AST-21_A01
AST-22	AST-22_A01
AST-23	AST-23_A01
AST-24	AST-24_A01
AST-24	AST-24_A02
AST-25	AST-25_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

AST-29	AST-29_A02
AST-29.1	AST-29.1_A01
AST-29.1	AST-29.1_A02
AST-30	AST-30_A01
AST-31	AST-31_A01
AST-31.1	AST-31.1_A01
BCD-01	BCD-01_A26
BCD-01	BCD-01_A27
BCD-01	BCD-01_A28
BCD-01	BCD-01_A29
BCD-01	BCD-01_A30
BCD-01	BCD-01_A31
BCD-01.1	BCD-01.1_A01
BCD-01.2	BCD-01.2_A01
BCD-01.3	BCD-01.3_A01
BCD-01.3	BCD-01.3_A02
BCD-01.4	BCD-01.4_A01
BCD-01.4	BCD-01.4_A02
BCD-01.4	BCD-01.4_A03
BCD-01.4	BCD-01.4_A04
BCD-01.4	BCD-01.4_A05
BCD-01.4	BCD-01.4_A06
BCD-02	BCD-02_A01
BCD-02	BCD-02_A02
BCD-02.1	BCD-02.1_A02
BCD-02.1	BCD-02.1_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

BCD-03	BCD-03_A01
BCD-03	BCD-03_A02
BCD-03	BCD-03_A03
BCD-03	BCD-03_A04
BCD-03	BCD-03_A05
BCD-03	BCD-03_A06
BCD-03	BCD-03_A07
BCD-03	BCD-03_A08
BCD-03	BCD-03_A09
BCD-03.1	BCD-03.1_A01
BCD-03.2	BCD-03.2_A01
BCD-04	BCD-04_A01
BCD-04	BCD-04_A02
BCD-04	BCD-04_A03
BCD-04	BCD-04_A04
BCD-04	BCD-04_A05
BCD-04	BCD-04_A06
BCD-04.1	BCD-04.1_A01
BCD-04.2	BCD-04.2_A01
BCD-04.2	BCD-04.2_A02
BCD-05	BCD-05_A01
BCD-05	BCD-05_A02
BCD-06	BCD-06_A01
BCD-06	BCD-06_A02
BCD-06	BCD-06_A03
BCD-06	BCD-06_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

BCD-06	BCD-06_A11
BCD-06	BCD-06_A12
BCD-06	BCD-06_A13
BCD-06	BCD-06_A14
BCD-06	BCD-06_A15
BCD-06	BCD-06_A16
BCD-06	BCD-06_A17
BCD-06	BCD-06_A18
BCD-06	BCD-06_A19
BCD-06	BCD-06_A20
BCD-06	BCD-06_A21
BCD-06	BCD-06_A22
BCD-06	BCD-06_A23
BCD-06	BCD-06_A24
BCD-06	BCD-06_A25
BCD-06	BCD-06_A26
BCD-06	BCD-06_A27
BCD-06	BCD-06_A28
BCD-06	BCD-06_A29
BCD-06	BCD-06_A30
BCD-06	BCD-06_A31
BCD-07	BCD-07_A01
BCD-07	BCD-07_A02
BCD-07	BCD-07_A03
BCD-08	BCD-08_A01
BCD-08	BCD-08_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

BCD-09	BCD-09_A02
BCD-09	BCD-09_A03
BCD-09	BCD-09_A04
BCD-09	BCD-09_A05
BCD-09	BCD-09_A06
BCD-09	BCD-09_A07
BCD-09.1	BCD-09.1_A01
BCD-09.2	BCD-09.2_A01
BCD-09.2	BCD-09.2_A02
BCD-09.3	BCD-09.3_A01
BCD-09.4	BCD-09.4_A01
BCD-09.5	BCD-09.5_A01
BCD-09.5	BCD-09.5_A02
BCD-10	BCD-10_A01
BCD-10	BCD-10_A02
BCD-10	BCD-10_A03
BCD-10	BCD-10_A04
BCD-10	BCD-10_A05
BCD-10	BCD-10_A06
BCD-10.1	BCD-10.1_A01
BCD-10.1	BCD-10.1_A02
BCD-10.1	BCD-10.1_A03
BCD-10.2	BCD-10.2_A01
BCD-10.3	BCD-10.3_A01
BCD-10.3	BCD-10.3_A02
BCD-10.3	BCD-10.3_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

BCD-11	BCD-11_A01
BCD-11	BCD-11_A02
BCD-11	BCD-11_A03
BCD-11	BCD-11_A04
BCD-11	BCD-11_A05
BCD-11	BCD-11_A06
BCD-11	BCD-11_A07
BCD-11	BCD-11_A08
BCD-11	BCD-11_A09
BCD-11	BCD-11_A10
BCD-11	BCD-11_A11
BCD-11.1	BCD-11.1_A01
BCD-11.1	BCD-11.1_A02
BCD-11.1	BCD-11.1_A03
BCD-11.1	BCD-11.1_A04
BCD-11.2	BCD-11.2_A01
BCD-11.2	BCD-11.2_A02
BCD-11.3	BCD-11.3_A01
BCD-11.3	BCD-11.3_A02
BCD-11.4	BCD-11.4_A01
BCD-11.4	BCD-11.4_A02
BCD-11.4	BCD-11.4_A03
BCD-11.5	BCD-11.5_A01
BCD-11.6	BCD-11.6_A01
BCD-11.6	BCD-11.6_A02
BCD-11.6	BCD-11.6_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

BCD-11.8	BCD-11.8_A04
BCD-11.9	BCD-11.9_A01
BCD-11.9	BCD-11.9_A02
BCD-11.10	BCD-11.10_A01
BCD-12	BCD-12_A01
BCD-12	BCD-12_A02
BCD-12.1	BCD-12.1_A01
BCD-12.2	BCD-12.2_A01
BCD-12.2	BCD-12.2_A02
BCD-12.2	BCD-12.2_A03
BCD-12.2	BCD-12.2_A04
BCD-12.3	BCD-12.3_A01
BCD-12.4	BCD-12.4_A01
BCD-12.4	BCD-12.4_A02
BCD-13	BCD-13_A01
BCD-14	BCD-14_A01
BCD-14	BCD-14_A02
BCD-15	BCD-15_A01
BCD-15	BCD-15_A02
BCD-15	BCD-15_A03
BCD-15	BCD-15_A04
BCD-15	BCD-15_A05
BCD-15	BCD-15_A06
BCD-15	BCD-15_A07
BCD-16	BCD-16_A01
BCD-16	BCD-16_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CAP-02	CAP-02_A04
CAP-02	CAP-02_A05
CAP-03	CAP-03_A01
CAP-03	CAP-03_A02
CAP-03	CAP-03_A03
CAP-04	CAP-04_A01
CAP-04	CAP-04_A02
CAP-04	CAP-04_A03
CHG-01	CHG-01_A01
CHG-01	CHG-01_A02
CHG-01	CHG-01_A03
CHG-01	CHG-01_A04
CHG-01	CHG-01_A05
CHG-01	CHG-01_A06
CHG-01	CHG-01_A07
CHG-01	CHG-01_A08
CHG-01	CHG-01_A09
CHG-01	CHG-01_A10
CHG-01	CHG-01_A11
CHG-01	CHG-01_A12
CHG-01	CHG-01_A13
CHG-01	CHG-01_A14
CHG-02	CHG-02_A01
CHG-02	CHG-02_A02
CHG-02	CHG-02_A03
CHG-02	CHG-02_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CHG-02.1	CHG-02.1_A07
CHG-02.1	CHG-02.1_A08
CHG-02.1	CHG-02.1_A09
CHG-02.1	CHG-02.1_A10
CHG-02.2	CHG-02.2_A01
CHG-02.2	CHG-02.2_A02
CHG-02.2	CHG-02.2_A03
CHG-02.2	CHG-02.2_A04
CHG-02.2	CHG-02.2_A05
CHG-02.2	CHG-02.2_A06
CHG-02.2	CHG-02.2_A07
CHG-02.2	CHG-02.2_A08
CHG-02.3	CHG-02.3_A01
CHG-02.3	CHG-02.3_A02
CHG-02.3	CHG-02.3_A03
CHG-02.3	CHG-02.3_A04
CHG-02.3	CHG-02.3_A05
CHG-02.4	CHG-02.4_A01
CHG-02.4	CHG-02.4_A02
CHG-02.4	CHG-02.4_A03
CHG-02.4	CHG-02.4_A04
CHG-02.4	CHG-02.4_A05
CHG-02.4	CHG-02.4_A06
CHG-02.4	CHG-02.4_A07
CHG-02.5	CHG-02.5_A01
CHG-02.5	CHG-02.5_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CHG-04	CHG-04_A04
CHG-04	CHG-04_A05
CHG-04	CHG-04_A06
CHG-04.1	CHG-04.1_A01
CHG-04.1	CHG-04.1_A02
CHG-04.1	CHG-04.1_A03
CHG-04.2	CHG-04.2_A01
CHG-04.2	CHG-04.2_A02
CHG-04.2	CHG-04.2_A03
CHG-04.2	CHG-04.2_A04
CHG-04.2	CHG-04.2_A05
CHG-04.2	CHG-04.2_A06
CHG-04.3	CHG-04.3_A01
CHG-04.3	CHG-04.3_A02
CHG-04.4	CHG-04.4_A01
CHG-04.4	CHG-04.4_A02
CHG-04.4	CHG-04.4_A03
CHG-04.4	CHG-04.4_A04
CHG-04.4	CHG-04.4_A05
CHG-04.4	CHG-04.4_A06
CHG-04.5	CHG-04.5_A01
CHG-05	CHG-05_A01
CHG-06	CHG-06_A01
CHG-06	CHG-06_A02
CHG-06	CHG-06_A03
CHG-06	CHG-06_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CHG-06.1	CHG-06.1_A02
CLD-01	CLD-01_A01
CLD-01	CLD-01_A02
CLD-01.1	CLD-01.1_A01
CLD-01.2	CLD-01.2_A01
CLD-02	CLD-02_A01
CLD-02	CLD-02_A02
CLD-03	CLD-03_A01
CLD-03	CLD-03_A02
CLD-03	CLD-03_A03
CLD-04	CLD-04_A01
CLD-04	CLD-04_A02
CLD-05	CLD-05_A01
CLD-05	CLD-05_A02
CLD-06	CLD-06_A01
CLD-06.1	CLD-06.1_A01
CLD-06.2	CLD-06.2_A01
CLD-06.3	CLD-06.3_A01
CLD-06.4	CLD-06.4_A01
CLD-07	CLD-07_A01
CLD-08	CLD-08_A01
CLD-08	CLD-08_A02
CLD-09	CLD-09_A01
CLD-09	CLD-09_A02
CLD-09	CLD-09_A03
CLD-09	CLD-09_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CPL-01.1	CPL-01.1_A01
CPL-01.1	CPL-01.1_A02
CPL-01.1	CPL-01.1_A03
CPL-01.1	CPL-01.1_A04
CPL-01.1	CPL-01.1_A05
CPL-01.2	CPL-01.2_A01
CPL-01.2	CPL-01.2_A02
CPL-02	CPL-02_A01
CPL-02	CPL-02_A02
CPL-02	CPL-02_A03
CPL-02	CPL-02_A04
CPL-02	CPL-02_A05
CPL-02	CPL-02_A06
CPL-02	CPL-02_A07
CPL-02	CPL-02_A08
CPL-02	CPL-02_A09
CPL-02	CPL-02_A10
CPL-02	CPL-02_A11
CPL-02	CPL-02_A12
CPL-02	CPL-02_A13
CPL-02	CPL-02_A14
CPL-02	CPL-02_A15
CPL-02	CPL-02_A16
CPL-02	CPL-02_A17
CPL-02	CPL-02_A18
CPL-02	CPL-02_A19

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CPL-02	CPL-02_A26
CPL-02	CPL-02_A27
CPL-02.1	CPL-02.1_A01
CPL-02.1	CPL-02.1_A02
CPL-02.1	CPL-02.1_A03
CPL-02.1	CPL-02.1_A04
CPL-03	CPL-03_A01
CPL-03	CPL-03_A02
CPL-03	CPL-03_A03
CPL-03	CPL-03_A04
CPL-03	CPL-03_A05
CPL-03	CPL-03_A06
CPL-03	CPL-03_A07
CPL-03	CPL-03_A08
CPL-03	CPL-03_A09
CPL-03.1	CPL-03.1_A01
CPL-03.2	CPL-03.2_A01
CPL-03.2	CPL-03.2_A02
CPL-03.2	CPL-03.2_A03
CPL-03.2	CPL-03.2_A04
CPL-04	CPL-04_A01
CPL-04	CPL-04_A02
CPL-05	CPL-05_A01
CPL-05	CPL-05_A02
CPL-05.1	CPL-05.1_A01
CPL-05.1	CPL-05.1_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CPL-06	CPL-06_A03
CPL-06	CPL-06_A04
CPL-06	CPL-06_A05
CPL-06	CPL-06_A06
CFG-01	CFG-01_A01
CFG-01	CFG-01_A02
CFG-01	CFG-01_A03
CFG-01	CFG-01_A04
CFG-01	CFG-01_A05
CFG-01	CFG-01_A06
CFG-01	CFG-01_A07
CFG-01	CFG-01_A08
CFG-01	CFG-01_A09
CFG-01	CFG-01_A10
CFG-01	CFG-01_A11
CFG-01	CFG-01_A12
CFG-01	CFG-01_A13
CFG-01	CFG-01_A14
CFG-01	CFG-01_A15
CFG-01	CFG-01_A16
CFG-01.1	CFG-01.1_A01
CFG-02	CFG-02_A01
CFG-02	CFG-02_A02
CFG-02	CFG-02_A03
CFG-02	CFG-02_A04
CFG-02	CFG-02_A05

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CFG-02.1	CFG-02.1_A03
CFG-02.1	CFG-02.1_A04
CFG-02.1	CFG-02.1_A05
CFG-02.2	CFG-02.2_A01
CFG-02.2	CFG-02.2_A02
CFG-02.2	CFG-02.2_A03
CFG-02.2	CFG-02.2_A04
CFG-02.3	CFG-02.3_A01
CFG-02.3	CFG-02.3_A02
CFG-02.4	CFG-02.4_A01
CFG-02.4	CFG-02.4_A02
CFG-02.5	CFG-02.5_A01
CFG-02.5	CFG-02.5_A02
CFG-02.5	CFG-02.5_A03
CFG-02.5	CFG-02.5_A04
CFG-02.6	CFG-02.6_A01
CFG-02.7	CFG-02.7_A01
CFG-02.7	CFG-02.7_A02
CFG-02.7	CFG-02.7_A03
CFG-02.7	CFG-02.7_A04
CFG-02.7	CFG-02.7_A05
CFG-02.7	CFG-02.7_A06
CFG-02.7	CFG-02.7_A07
CFG-02.7	CFG-02.7_A08
CFG-02.8	CFG-02.8_A01
CFG-02.8	CFG-02.8_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CFG-03	CFG-03_A05
CFG-03	CFG-03_A06
CFG-03	CFG-03_A07
CFG-03	CFG-03_A08
CFG-03	CFG-03_A09
CFG-03	CFG-03_A10
CFG-03	CFG-03_A11
CFG-03	CFG-03_A12
CFG-03.1	CFG-03.1_A01
CFG-03.1	CFG-03.1_A02
CFG-03.1	CFG-03.1_A03
CFG-03.1	CFG-03.1_A04
CFG-03.1	CFG-03.1_A05
CFG-03.1	CFG-03.1_A06
CFG-03.1	CFG-03.1_A07
CFG-03.1	CFG-03.1_A08
CFG-03.1	CFG-03.1_A09
CFG-03.1	CFG-03.1_A10
CFG-03.1	CFG-03.1_A11
CFG-03.1	CFG-03.1_A12
CFG-03.1	CFG-03.1_A13
CFG-03.1	CFG-03.1_A14
CFG-03.1	CFG-03.1_A15
CFG-03.1	CFG-03.1_A16
CFG-03.1	CFG-03.1_A17
CFG-03.1	CFG-03.1_A18

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CFG-03.1	CFG-03.1_A25
CFG-03.1	CFG-03.1_A26
CFG-03.2	CFG-03.2_A01
CFG-03.2	CFG-03.2_A02
CFG-03.3	CFG-03.3_A01
CFG-03.3	CFG-03.3_A02
CFG-03.3	CFG-03.3_A03
CFG-03.3	CFG-03.3_A04
CFG-03.3	CFG-03.3_A05
CFG-03.3	CFG-03.3_A06
CFG-03.3	CFG-03.3_A07
CFG-03.3	CFG-03.3_A08
CFG-03.3	CFG-03.3_A09
CFG-03.3	CFG-03.3_A10
CFG-03.3	CFG-03.3_A11
CFG-03.3	CFG-03.3_A12
CFG-03.3	CFG-03.3_A13
CFG-03.3	CFG-03.3_A14
CFG-03.3	CFG-03.3_A15
CFG-03.3	CFG-03.3_A16
CFG-03.4	CFG-03.4_A01
CFG-03.4	CFG-03.4_A02
CFG-04	CFG-04_A01
CFG-04	CFG-04_A02
CFG-04	CFG-04_A03
CFG-04.1	CFG-04.1_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CFG-05	CFG-05_A02
CFG-05	CFG-05_A03
CFG-05	CFG-05_A04
CFG-05.1	CFG-05.1_A01
CFG-05.1	CFG-05.1_A02
CFG-05.1	CFG-05.1_A03
CFG-05.2	CFG-05.2_A01
CFG-06	CFG-06_A01
CFG-06	CFG-06_A02
CFG-06	CFG-06_A03
CFG-06	CFG-06_A04
CFG-06	CFG-06_A05
CFG-06	CFG-06_A06
CFG-07	CFG-07_A01
CFG-07	CFG-07_A02
CFG-08	CFG-08_A01
CFG-08	CFG-08_A02
CFG-08.1	CFG-08.1_A01
MON-01	MON-01_A01
MON-01	MON-01_A02
MON-01	MON-01_A03
MON-01	MON-01_A04
MON-01	MON-01_A05
MON-01	MON-01_A06
MON-01	MON-01_A07
MON-01	MON-01_A08

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MON-01.3	MON-01.3_A02
MON-01.3	MON-01.3_A03
MON-01.3	MON-01.3_A04
MON-01.3	MON-01.3_A05
MON-01.3	MON-01.3_A06
MON-01.3	MON-01.3_A07
MON-01.3	MON-01.3_A08
MON-01.4	MON-01.4_A01
MON-01.4	MON-01.4_A02
MON-01.4	MON-01.4_A03
MON-01.5	MON-01.5_A01
MON-01.5	MON-01.5_A02
MON-01.5	MON-01.5_A03
MON-01.5	MON-01.5_A04
MON-01.6	MON-01.6_A01
MON-01.6	MON-01.6_A02
MON-01.6	MON-01.6_A03
MON-01.7	MON-01.7_A01
MON-01.7	MON-01.7_A02
MON-01.7	MON-01.7_A03
MON-01.7	MON-01.7_A04
MON-01.7	MON-01.7_A05
MON-01.8	MON-01.8_A01
MON-01.8	MON-01.8_A02
MON-01.8	MON-01.8_A03
MON-01.8	MON-01.8_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MON-01.11	MON-01.11_A02
MON-01.11	MON-01.11_A03
MON-01.11	MON-01.11_A04
MON-01.11	MON-01.11_A05
MON-01.11	MON-01.11_A06
MON-01.12	MON-01.12_A01
MON-01.12	MON-01.12_A02
MON-01.12	MON-01.12_A03
MON-01.12	MON-01.12_A04
MON-01.13	MON-01.13_A01
MON-01.13	MON-01.13_A02
MON-01.13	MON-01.13_A03
MON-01.13	MON-01.13_A04
MON-01.13	MON-01.13_A05
MON-01.13	MON-01.13_A06
MON-01.14	MON-01.14_A01
MON-01.14	MON-01.14_A02
MON-01.14	MON-01.14_A03
MON-01.15	MON-01.15_A01
MON-01.15	MON-01.15_A02
MON-01.16	MON-01.16_A01
MON-01.16	MON-01.16_A02
MON-01.17	MON-01.17_A01
MON-01.17	MON-01.17_A02
MON-02	MON-02_A01
MON-02	MON-02_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MON-02	MON-02_A09
MON-02.1	MON-02.1_A01
MON-02.1	MON-02.1_A02
MON-02.1	MON-02.1_A03
MON-02.1	MON-02.1_A04
MON-02.1	MON-02.1_A05
MON-02.1	MON-02.1_A06
MON-02.2	MON-02.2_A01
MON-02.2	MON-02.2_A02
MON-02.3	MON-02.3_A01
MON-02.3	MON-02.3_A02
MON-02.3	MON-02.3_A03
MON-02.4	MON-02.4_A01
MON-02.5	MON-02.5_A01
MON-02.6	MON-02.6_A01
MON-02.6	MON-02.6_A02
MON-02.6	MON-02.6_A03
MON-02.6	MON-02.6_A04
MON-02.6	MON-02.6_A05
MON-02.6	MON-02.6_A06
MON-02.7	MON-02.7_A01
MON-02.7	MON-02.7_A02
MON-02.7	MON-02.7_A03
MON-02.8	MON-02.8_A01
MON-02.8	MON-02.8_A02
MON-02.8	MON-02.8_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MON-03	MON-03_A05
MON-03	MON-03_A06
MON-03	MON-03_A07
MON-03	MON-03_A08
MON-03	MON-03_A09
MON-03	MON-03_A10
MON-03	MON-03_A11
MON-03.1	MON-03.1_A01
MON-03.1	MON-03.1_A02
MON-03.2	MON-03.2_A01
MON-03.2	MON-03.2_A02
MON-03.2	MON-03.2_A03
MON-03.3	MON-03.3_A01
MON-03.4	MON-03.4_A01
MON-03.4	MON-03.4_A02
MON-03.5	MON-03.5_A01
MON-03.5	MON-03.5_A02
MON-03.6	MON-03.6_A01
MON-03.6	MON-03.6_A02
MON-03.7	MON-03.7_A01
MON-03.7	MON-03.7_A02
MON-04	MON-04_A01
MON-04	MON-04_A02
MON-05	MON-05_A01
MON-05	MON-05_A02
MON-05	MON-05_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MON-05.2	MON-05.2_A01
MON-05.2	MON-05.2_A02
MON-05.2	MON-05.2_A03
MON-05.2	MON-05.2_A04
MON-06	MON-06_A01
MON-06	MON-06_A02
MON-06	MON-06_A03
MON-06	MON-06_A04
MON-06	MON-06_A05
MON-06	MON-06_A06
MON-06.1	MON-06.1_A01
MON-06.1	MON-06.1_A02
MON-06.2	MON-06.2_A01
MON-06.2	MON-06.2_A02
MON-06.2	MON-06.2_A03
MON-07	MON-07_A01
MON-07	MON-07_A02
MON-07.1	MON-07.1_A01
MON-07.1	MON-07.1_A02
MON-07.1	MON-07.1_A03
MON-07.1	MON-07.1_A04
MON-07.1	MON-07.1_A05
MON-08	MON-08_A01
MON-08	MON-08_A02
MON-08	MON-08_A03
MON-08	MON-08_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MON-08.1	MON-08.1_A03
MON-08.2	MON-08.2_A01
MON-08.2	MON-08.2_A02
MON-08.3	MON-08.3_A01
MON-08.4	MON-08.4_A01
MON-08.4	MON-08.4_A02
MON-09	MON-09_A01
MON-09	MON-09_A02
MON-09.1	MON-09.1_A01
MON-09.1	MON-09.1_A02
MON-09.1	MON-09.1_A03
MON-09.1	MON-09.1_A04
MON-09.1	MON-09.1_A05
MON-09.1	MON-09.1_A06
MON-09.1	MON-09.1_A07
MON-10	MON-10_A01
MON-10	MON-10_A02
MON-11	MON-11_A01
MON-11	MON-11_A02
MON-11	MON-11_A03
MON-11	MON-11_A04
MON-11	MON-11_A05
MON-11	MON-11_A06
MON-11.1	MON-11.1_A01
MON-11.1	MON-11.1_A02
MON-11.1	MON-11.1_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MON-11.2	MON-11.2_A06
MON-11.3	MON-11.3_A01
MON-11.3	MON-11.3_A02
MON-11.3	MON-11.3_A03
MON-11.3	MON-11.3_A04
MON-11.3	MON-11.3_A05
MON-11.3	MON-11.3_A06
MON-11.3	MON-11.3_A07
MON-11.3	MON-11.3_A08
MON-11.3	MON-11.3_A09
MON-11.3	MON-11.3_A10
MON-11.3	MON-11.3_A11
MON-11.3	MON-11.3_A12
MON-11.3	MON-11.3_A13
MON-11.3	MON-11.3_A14
MON-11.3	MON-11.3_A15
MON-11.3	MON-11.3_A16
MON-12	MON-12_A01
MON-12	MON-12_A02
MON-12	MON-12_A03
MON-12	MON-12_A04
MON-12	MON-12_A05
MON-12	MON-12_A06
MON-12	MON-12_A07
MON-12	MON-12_A08
MON-13	MON-13_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MON-14.1	MON-14.1_A03
MON-15	MON-15_A01
MON-15	MON-15_A02
MON-16	MON-16_A01
MON-16	MON-16_A02
MON-16	MON-16_A03
MON-16	MON-16_A04
MON-16	MON-16_A05
MON-16	MON-16_A06
MON-16	MON-16_A07
MON-16	MON-16_A08
MON-16	MON-16_A09
MON-16	MON-16_A10
MON-16	MON-16_A11
MON-16.1	MON-16.1_A01
MON-16.1	MON-16.1_A02
MON-16.1	MON-16.1_A03
MON-16.2	MON-16.2_A01
MON-16.2	MON-16.2_A02
MON-16.2	MON-16.2_A03
MON-16.3	MON-16.3_A01
MON-16.3	MON-16.3_A02
MON-16.3	MON-16.3_A03
MON-16.3	MON-16.3_A04
MON-16.3	MON-16.3_A05
MON-16.4	MON-16.4_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CRY-01	CRY-01.1_A03
CRY-01	CRY-01.1_A04
CRY-01	CRY-01.1_A05
CRY-01	CRY-01.1_A06
CRY-01	CRY-01.1_A07
CRY-01	CRY-01.1_A08
CRY-01.2	CRY-01.2_A01
CRY-01.2	CRY-01.2_A02
CRY-01.2	CRY-01.2_A03
CRY-01.3	CRY-01.3_A01
CRY-01.3	CRY-01.3_A02
CRY-01.3	CRY-01.3_A03
CRY-01.3	CRY-01.3_A04
CRY-01.4	CRY-01.4_A01
CRY-01.4	CRY-01.4_A02
CRY-01.5	CRY-01.5_A01
CRY-01.5	CRY-01.5_A02
CRY-01.5	CRY-01.5_A03
CRY-01.5	CRY-01.5_A04
CRY-01.5	CRY-01.5_A05
CRY-02	CRY-02_A01
CRY-03	CRY-03_A01
CRY-04	CRY-04_A01
CRY-04	CRY-04_A02
CRY-04	CRY-04_A03
CRY-04	CRY-04_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CRY-05	CRY-05_A03
CRY-05	CRY-05_A04
CRY-05	CRY-05_A05
CRY-05.1	CRY-05.1_A01
CRY-05.1	CRY-05.1_A02
CRY-05.2	CRY-05.2_A01
CRY-05.2	CRY-05.2_A02
CRY-05.2	CRY-05.2_A03
CRY-05.2	CRY-05.2_A04
CRY-05.2	CRY-05.2_A05
CRY-05.2	CRY-05.2_A06
CRY-05.3	CRY-05.3_A01
CRY-06	CRY-06_A01
CRY-07	CRY-07_A01
CRY-07	CRY-07_A02
CRY-07	CRY-07_A03
CRY-08	CRY-08_A01
CRY-08	CRY-08_A02
CRY-08	CRY-08_A03
CRY-08	CRY-08_A04
CRY-08	CRY-08_A05
CRY-08	CRY-08_A06
CRY-08.1	CRY-08.1_A01
CRY-09	CRY-09_A01
CRY-09	CRY-09_A02
CRY-09.1	CRY-09.1_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

CRY-09.3	CRY-09.3_A01
CRY-09.4	CRY-09.4_A01
CRY-09.5	CRY-09.5_A01
CRY-09.6	CRY-09.6_A01
CRY-09.7	CRY-09.7_A01
CRY-10	CRY-10_A01
CRY-10	CRY-10_A02
CRY-10	CRY-10_A03
CRY-10	CRY-10_A04
CRY-11	CRY-11_A01
CRY-11	CRY-11_A02
DCH-01	DCH-01_A01
DCH-01	DCH-01_A02
DCH-01	DCH-01_A03
DCH-01	DCH-01_A04
DCH-01.1	DCH-01.1_A01
DCH-01.1	DCH-01.1_A02
DCH-01.2	DCH-01.2_A01
DCH-01.2	DCH-01.2_A02
DCH-01.2	DCH-01.2_A03
DCH-01.3	DCH-01.3_A01
DCH-02	DCH-02_A01
DCH-02	DCH-02_A02
DCH-02.1	DCH-02.1_A01
DCH-02.1	DCH-02.1_A02
DCH-03	DCH-03_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-03.1	DCH-03.1_A02
DCH-03.2	DCH-03.2_A01
DCH-03.3	DCH-03.3_A01
DCH-03.3	DCH-03.3_A02
DCH-03.3	DCH-03.3_A03
DCH-03.3	DCH-03.3_A04
DCH-03.3	DCH-03.3_A05
DCH-04	DCH-04_A01
DCH-04	DCH-04_A02
DCH-04	DCH-04_A03
DCH-04	DCH-04_A04
DCH-04	DCH-04_A05
DCH-04.1	DCH-04.1_A01
DCH-05	DCH-05_A01
DCH-05	DCH-05_A02
DCH-05	DCH-05_A03
DCH-05	DCH-05_A04
DCH-05	DCH-05_A05
DCH-05	DCH-05_A06
DCH-05	DCH-05_A07
DCH-05	DCH-05_A08
DCH-05	DCH-05_A09
DCH-05.1	DCH-05.1_A01
DCH-05.1	DCH-05.1_A02
DCH-05.1	DCH-05.1_A03
DCH-05.1	DCH-05.1_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-05.2	DCH-05.2_A01
DCH-05.2	DCH-05.2_A02
DCH-05.3	DCH-05.3_A01
DCH-05.3	DCH-05.3_A02
DCH-05.3	DCH-05.3_A03
DCH-05.3	DCH-05.3_A04
DCH-05.3	DCH-05.3_A05
DCH-05.3	DCH-05.3_A06
DCH-05.3	DCH-05.3_A07
DCH-05.3	DCH-05.3_A08
DCH-05.3	DCH-05.3_A09
DCH-05.3	DCH-05.3_A10
DCH-05.4	DCH-05.4_A01
DCH-05.4	DCH-05.4_A02
DCH-05.4	DCH-05.4_A03
DCH-05.4	DCH-05.4_A04
DCH-05.4	DCH-05.4_A05
DCH-05.4	DCH-05.4_A06
DCH-05.4	DCH-05.4_A07
DCH-05.4	DCH-05.4_A08
DCH-05.4	DCH-05.4_A09
DCH-05.4	DCH-05.4_A10
DCH-05.4	DCH-05.4_A11
DCH-05.4	DCH-05.4_A12
DCH-05.5	DCH-05.5_A01
DCH-05.5	DCH-05.5_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-05.6	DCH-05.6_A05
DCH-05.6	DCH-05.6_A06
DCH-05.6	DCH-05.6_A07
DCH-05.6	DCH-05.6_A08
DCH-05.6	DCH-05.6_A09
DCH-05.6	DCH-05.6_A10
DCH-05.6	DCH-05.6_A11
DCH-05.6	DCH-05.6_A12
DCH-05.6	DCH-05.6_A13
DCH-05.6	DCH-05.6_A14
DCH-05.7	DCH-05.7_A01
DCH-05.7	DCH-05.7_A02
DCH-05.8	DCH-05.8_A01
DCH-05.8	DCH-05.8_A02
DCH-05.8	DCH-05.8_A03
DCH-05.8	DCH-05.8_A04
DCH-05.9	DCH-05.9_A01
DCH-05.9	DCH-05.9_A02
DCH-05.9	DCH-05.9_A03
DCH-05.9	DCH-05.9_A04
DCH-05.10	DCH-05.10_A01
DCH-05.10	DCH-05.10_A02
DCH-05.11	DCH-05.11_A01
DCH-05.11	DCH-05.11_A02
DCH-06	DCH-06_A01
DCH-06	DCH-06_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-06.1	DCH-06.1_A02
DCH-06.1	DCH-06.1_A03
DCH-06.1	DCH-06.1_A04
DCH-06.1	DCH-06.1_A05
DCH-06.2	DCH-06.2_A01
DCH-06.2	DCH-06.2_A02
DCH-06.3	DCH-06.3_A01
DCH-06.3	DCH-06.3_A02
DCH-06.4	DCH-06.4_A01
DCH-06.4	DCH-06.4_A02
DCH-06.5	DCH-06.5_A01
DCH-06.5	DCH-06.5_A02
DCH-07	DCH-07_A01
DCH-07	DCH-07_A02
DCH-07	DCH-07_A03
DCH-07	DCH-07_A04
DCH-07	DCH-07_A05
DCH-07	DCH-07_A06
DCH-07	DCH-07_A07
DCH-07	DCH-07_A08
DCH-07	DCH-07_A09
DCH-07	DCH-07_A10
DCH-07	DCH-07_A11
DCH-07.1	DCH-07.1_A01
DCH-07.1	DCH-07.1_A02
DCH-07.2	DCH-07.2_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-08	DCH-08_A05
DCH-08	DCH-08_A06
DCH-08	DCH-08_A07
DCH-08	DCH-08_A08
DCH-08	DCH-08_A09
DCH-08	DCH-08_A10
DCH-09	DCH-09_A01
DCH-09	DCH-09_A02
DCH-09	DCH-09_A03
DCH-09	DCH-09_A04
DCH-09	DCH-09_A05
DCH-09	DCH-09_A06
DCH-09	DCH-09_A07
DCH-09	DCH-09_A08
DCH-09	DCH-09_A09
DCH-09	DCH-09_A10
DCH-09	DCH-09_A11
DCH-09	DCH-09_A12
DCH-09	DCH-09_A13
DCH-09	DCH-09_A14
DCH-09.1	DCH-09.1_A01
DCH-09.1	DCH-09.1_A02
DCH-09.1	DCH-09.1_A03
DCH-09.1	DCH-09.1_A04
DCH-09.1	DCH-09.1_A05
DCH-09.2	DCH-09.2_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-09.3	DCH-09.3_A04
DCH-09.3	DCH-09.3_A05
DCH-09.3	DCH-09.3_A06
DCH-09.4	DCH-09.4_A01
DCH-09.4	DCH-09.4_A02
DCH-09.5	DCH-09.5_A01
DCH-09.5	DCH-09.5_A02
DCH-10	DCH-10_A01
DCH-10	DCH-10_A02
DCH-10	DCH-10_A03
DCH-10	DCH-10_A04
DCH-10	DCH-10_A05
DCH-10	DCH-10_A06
DCH-10.1	DCH-10.1_A01
DCH-10.1	DCH-10.1_A02
DCH-10.2	DCH-10.2_A01
DCH-11	DCH-11_A01
DCH-11	DCH-11_A02
DCH-11	DCH-11_A03
DCH-11	DCH-11_A04
DCH-11	DCH-11_A05
DCH-11	DCH-11_A06
DCH-11	DCH-11_A07
DCH-11	DCH-11_A08
DCH-11	DCH-11_A09
DCH-11	DCH-11_A10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-13	DCH-13_A06
DCH-13	DCH-13_A07
DCH-13	DCH-13_A08
DCH-13	DCH-13_A09
DCH-13	DCH-13_A10
DCH-13	DCH-13_A11
DCH-13	DCH-13_A12
DCH-13.1	DCH-13.1_A01
DCH-13.1	DCH-13.1_A02
DCH-13.2	DCH-13.2_A01
DCH-13.2	DCH-13.2_A02
DCH-13.2	DCH-13.2_A03
DCH-13.2	DCH-13.2_A04
DCH-13.2	DCH-13.2_A05
DCH-13.3	DCH-13.3_A02
DCH-13.3	DCH-13.3_A03
DCH-13.3	DCH-13.3_A04
DCH-13.3	DCH-13.3_A06
DCH-13.4	DCH-13.4_A01
DCH-13.4	DCH-13.4_A02
DCH-13.4	DCH-13.4_A03
DCH-13.4	DCH-13.4_A04
DCH-14	DCH-14_A01
DCH-14	DCH-14_A02
DCH-14	DCH-14_A03
DCH-14.1	DCH-14.1_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-15	DCH-15_A04
DCH-15	DCH-15_A05
DCH-15	DCH-15_A06
DCH-15	DCH-15_A07
DCH-16	DCH-16_A01
DCH-16	DCH-16_A02
DCH-16	DCH-16_A03
DCH-17	DCH-17_A01
DCH-18	DCH-18_A01
DCH-18	DCH-18_A02
DCH-18	DCH-18_A03
DCH-18	DCH-18_A04
DCH-18	DCH-18_A05
DCH-18	DCH-18_A06
DCH-18	DCH-18_A07
DCH-18	DCH-18_A08
DCH-18.1	DCH-18.1_A01
DCH-18.1	DCH-18.1_A02
DCH-18.2	DCH-18.2_A01
DCH-18.2	DCH-18.2_A02
DCH-18.2	DCH-18.2_A03
DCH-18.2	DCH-18.2_A04
DCH-18.2	DCH-18.2_A05
DCH-18.2	DCH-18.2_A06
DCH-18.2	DCH-18.2_A07
DCH-18.2	DCH-18.2_A08

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-20	DCH-20_A01
DCH-21	DCH-21_A01
DCH-21	DCH-21_A02
DCH-21	DCH-21_A03
DCH-21	DCH-21_A04
DCH-21	DCH-21_A05
DCH-21	DCH-21_A06
DCH-22	DCH-22_A01
DCH-22	DCH-22_A02
DCH-22	DCH-22_A03
DCH-22	DCH-22_A04
DCH-22	DCH-22_A05
DCH-22	DCH-22_A06
DCH-22	DCH-22_A07
DCH-22	DCH-22_A08
DCH-22	DCH-22_A09
DCH-22	DCH-22_A10
DCH-22	DCH-22_A11
DCH-22	DCH-22_A12
DCH-22	DCH-22_A13
DCH-22	DCH-22_A14
DCH-22	DCH-22_A15
DCH-22	DCH-22_A16
DCH-22	DCH-22_A17
DCH-22	DCH-22_A18
DCH-22	DCH-22_A19

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-22	DCH-22_A26
DCH-22	DCH-22_A27
DCH-22.1	DCH-22.1_A01
DCH-22.1	DCH-22.1_A02
DCH-22.1	DCH-22.1_A03
DCH-22.1	DCH-22.1_A04
DCH-22.1	DCH-22.1_A05
DCH-22.2	DCH-22.2_A01
DCH-22.2	DCH-22.2_A02
DCH-22.2	DCH-22.2_A03
DCH-22.2	DCH-22.2_A04
DCH-22.2	DCH-22.2_A05
DCH-22.2	DCH-22.2_A06
DCH-22.3	DCH-22.3_A01
DCH-23	DCH-23_A01
DCH-23	DCH-23_A02
DCH-23	DCH-23_A03
DCH-23	DCH-23_A04
DCH-23.1	DCH-23.1_A01
DCH-23.2	DCH-23.2_A01
DCH-23.3	DCH-23.3_A01
DCH-23.4	DCH-23.4_A01
DCH-23.5	DCH-23.5_A01
DCH-23.5	DCH-23.5_A02
DCH-23.5	DCH-23.5_A03
DCH-23.6	DCH-23.6_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DCH-24	DCH-24_A03
DCH-24	DCH-24_A04
DCH-24	DCH-24_A05
DCH-24	DCH-24_A06
DCH-24	DCH-24_A07
DCH-24	DCH-24_A08
DCH-24.1	DCH-24.1_A01
DCH-24.1	DCH-24.1_A02
DCH-24.1	DCH-24.1_A03
DCH-25	DCH-25_A01
DCH-25	DCH-25_A02
DCH-25	DCH-25_A03
DCH-25.1	DCH-25.1_A01
DCH-25.1	DCH-25.1_A02
DCH-26	DCH-26_A01
DCH-26	DCH-26_A02
DCH-26	DCH-26_A03
DCH-26	DCH-26_A04
EMB-01	EMB-01_A01
EMB-01	EMB-01_A02
EMB-01	EMB-01_A03
EMB-01	EMB-01_A04
EMB-02	EMB-02_A01
EMB-03	EMB-03_A01
EMB-04	EMB-04_A01
EMB-05	EMB-05_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

EMB-11	EMB-11_A01
EMB-12	EMB-12_A01
EMB-13	EMB-13_A01
EMB-14	EMB-14_A01
EMB-15	EMB-15_A01
EMB-16	EMB-16_A01
EMB-17	EMB-17_A01
EMB-18	EMB-18_A01
EMB-19	EMB-19_A01
END-01	END-01_A01
END-01	END-01_A02
END-01	END-01_A03
END-01	END-01_A04
END-01	END-01_A05
END-01	END-01_A06
END-01	END-01_A07
END-01	END-01_A08
END-01	END-01_A09
END-02	END-02_A01
END-02	END-02_A03
END-02	END-02_A04
END-03	END-03_A01
END-03	END-03_A02
END-03	END-03_A03
END-03	END-03_A04
END-03	END-03_A05

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

END-03.1	END-03.1_A06
END-03.1	END-03.1_A07
END-03.1	END-03.1_A08
END-03.1	END-03.1_A09
END-03.1	END-03.1_A10
END-03.1	END-03.1_A11
END-03.1	END-03.1_A12
END-03.1	END-03.1_A13
END-03.2	END-03.2_A01
END-03.2	END-03.2_A02
END-03.2	END-03.2_A03
END-03.2	END-03.2_A04
END-03.2	END-03.2_A05
END-03.2	END-03.2_A06
END-04	END-04_A01
END-04	END-04_A02
END-04	END-04_A03
END-04	END-04_A04
END-04	END-04_A05
END-04	END-04_A06
END-04	END-04_A07
END-04	END-04_A08
END-04	END-04_A09
END-04	END-04_A10
END-04	END-04_A11
END-04	END-04_A12

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

END-04.2	END-04.2_A01
END-04.3	END-04.3_A01
END-04.3	END-04.3_A02
END-04.4	END-04.4_A01
END-04.4	END-04.4_A02
END-04.4	END-04.4_A03
END-04.4	END-04.4_A04
END-04.5	END-04.5_A01
END-04.5	END-04.5_A02
END-04.5	END-04.5_A03
END-04.5	END-04.5_A04
END-04.6	END-04.6_A01
END-04.6	END-04.6_A02
END-04.7	END-04.7_A01
END-05	END-05_A01
END-06	END-06_A01
END-06	END-06_A02
END-06	END-06_A03
END-06	END-06_A04
END-06	END-06_A05
END-06	END-06_A06
END-06	END-06_A07
END-06	END-06_A08
END-06	END-06_A09
END-06	END-06_A10
END-06	END-06_A11

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

END-06.1	END-06.1_A06
END-06.1	END-06.1_A07
END-06.1	END-06.1_A08
END-06.1	END-06.1_A09
END-06.1	END-06.1_A10
END-06.1	END-06.1_A11
END-06.1	END-06.1_A12
END-06.2	END-06.2_A01
END-06.2	END-06.2_A02
END-06.3	END-06.3_A01
END-06.3	END-06.3_A02
END-06.4	END-06.4_A01
END-06.4	END-06.4_A02
END-06.5	END-06.5_A01
END-06.5	END-06.5_A02
END-06.6	END-06.6_A01
END-06.6	END-06.6_A02
END-06.6	END-06.6_A03
END-06.7	END-06.7_A01
END-06.7	END-06.7_A02
END-06.7	END-06.7_A03
END-07	END-07_A01
END-07	END-07_A02
END-08	END-08_A01
END-08	END-08_A02
END-08	END-08_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

END-09	END-09_A02
END-09	END-09_A03
END-10	END-10_A01
END-10	END-10_A02
END-10	END-10_A03
END-10	END-10_A04
END-10	END-10_A05
END-10	END-10_A06
END-10	END-10_A07
END-10	END-10_A08
END-10	END-10_A09
END-10	END-10_A10
END-10	END-10_A11
END-10	END-10_A12
END-10	END-10_A13
END-10	END-10_A14
END-10	END-10_A15
END-10	END-10_A16
END-10	END-10_A17
END-10	END-10_A18
END-10	END-10_A19
END-10	END-10_A20
END-10	END-10_A21
END-11	END-11_A01
END-11	END-11_A02
END-11	END-11_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

END-13	END-13_A01
END-13	END-13_A02
END-13	END-13_A03
END-13	END-13_A04
END-13	END-13_A05
END-13	END-13_A06
END-13.1	END-13.1_A01
END-13.1	END-13.1_A02
END-13.2	END-13.2_A01
END-13.2	END-13.2_A02
END-13.2	END-13.2_A03
END-13.3	END-13.3_A01
END-13.3	END-13.3_A02
END-13.3	END-13.3_A03
END-13.3	END-13.3_A04
END-13.3	END-13.3_A05
END-13.3	END-13.3_A06
END-13.3	END-13.3_A07
END-13.3	END-13.3_A08
END-13.3	END-13.3_A09
END-13.3	END-13.3_A10
END-13.3	END-13.3_A11
END-13.3	END-13.3_A12
END-13.3	END-13.3_A13
END-13.3	END-13.3_A14
END-13.3	END-13.3_A15

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

END-13.3	END-13.3_A22
END-13.3	END-13.3_A23
END-13.3	END-13.3_A24
END-13.3	END-13.3_A25
END-13.3	END-13.3_A26
END-13.3	END-13.3_A27
END-13.3	END-13.3_A28
END-13.3	END-13.3_A29
END-13.3	END-13.3_A30
END-13.4	END-13.4_A01
END-13.4	END-13.4_A02
END-14	END-14_A01
END-14	END-14_A02
END-14	END-14_A03
END-14	END-14_A04
END-14	END-14_A05
END-14	END-14_A06
END-14	END-14_A07
END-14	END-14_A08
END-14.1	END-14.1_A01
END-14.1	END-14.1_A02
END-14.1	END-14.1_A03
END-14.2	END-14.2_A01
END-14.2	END-14.2_A02
END-15	END-15_A01
END-16	END-16_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

HRS-01	HRS-01_A04
HRS-01	HRS-01_A05
HRS-01	HRS-01_A06
HRS-01	HRS-01_A07
HRS-01	HRS-01_A08
HRS-01	HRS-01_A09
HRS-01	HRS-01_A10
HRS-01	HRS-01_A11
HRS-01	HRS-01_A12
HRS-01	HRS-01_A13
HRS-01	HRS-01_A14
HRS-01	HRS-01_A15
HRS-01	HRS-01_A16
HRS-01	HRS-01_A17
HRS-01	HRS-01_A18
HRS-01	HRS-01_A19
HRS-01	HRS-01_A20
HRS-01	HRS-01_A21
HRS-01	HRS-01_A22
HRS-01	HRS-01_A23
HRS-01	HRS-01_A24
HRS-01	HRS-01_A25
HRS-01	HRS-01_A26
HRS-01	HRS-01_A27
HRS-01	HRS-01_A28
HRS-02	HRS-02_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

HRS-02.2	HRS-02.2_A03
HRS-03	HRS-03_A01
HRS-03	HRS-03_A02
HRS-03.1	HRS-03.1_A01
HRS-03.1	HRS-03.1_A02
HRS-03.2	HRS-03.2_A01
HRS-03.2	HRS-03.2_A02
HRS-03.2	HRS-03.2_A03
HRS-03.2	HRS-03.2_A04
HRS-04	HRS-04_A01
HRS-04	HRS-04_A02
HRS-04	HRS-04_A03
HRS-04	HRS-04_A04
HRS-04	HRS-04_A05
HRS-04	HRS-04_A06
HRS-04.1	HRS-04.1_A01
HRS-04.1	HRS-04.1_A02
HRS-04.1	HRS-04.1_A03
HRS-04.1	HRS-04.1_A04
HRS-04.1	HRS-04.1_A05
HRS-04.1	HRS-04.1_A06
HRS-04.1	HRS-04.1_A07
HRS-04.1	HRS-04.1_A08
HRS-04.1	HRS-04.1_A09
HRS-04.1	HRS-04.1_A10
HRS-04.1	HRS-04.1_A11

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

HRS-04.3	HRS-04.3_A02
HRS-04.3	HRS-04.3_A03
HRS-04.4	HRS-04.4_A01
HRS-04.4	HRS-04.4_A02
HRS-05	HRS-05_A01
HRS-05.1	HRS-05.1_A01
HRS-05.1	HRS-05.1_A02
HRS-05.1	HRS-05.1_A03
HRS-05.1	HRS-05.1_A04
HRS-05.1	HRS-05.1_A05
HRS-05.1	HRS-05.1_A06
HRS-05.2	HRS-05.2_A01
HRS-05.2	HRS-05.2_A02
HRS-05.2	HRS-05.2_A03
HRS-05.3	HRS-05.3_A01
HRS-05.3	HRS-05.3_A02
HRS-05.4	HRS-05.4_A01
HRS-05.4	HRS-05.4_A02
HRS-05.5	HRS-05.5_A01
HRS-05.5	HRS-05.5_A02
HRS-05.6	HRS-05.6_A01
HRS-05.7	HRS-05.7_A01
HRS-05.7	HRS-05.7_A02
HRS-06	HRS-06_A01
HRS-06	HRS-06_A02
HRS-06	HRS-06_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

HRS-06.1	HRS-06.1_A04
HRS-06.1	HRS-06.1_A05
HRS-06.1	HRS-06.1_A06
HRS-06.1	HRS-06.1_A07
HRS-06.1	HRS-06.1_A08
HRS-06.1	HRS-06.1_A09
HRS-06.2	HRS-06.2_A01
HRS-06.2	HRS-06.2_A02
HRS-07	HRS-07_A01
HRS-07	HRS-07_A02
HRS-07	HRS-07_A03
HRS-07	HRS-07_A04
HRS-07	HRS-07_A05
HRS-07	HRS-07_A06
HRS-07	HRS-07_A07
HRS-07	HRS-07_A08
HRS-07	HRS-07_A09
HRS-07	HRS-07_A10
HRS-07	HRS-07_A11
HRS-07.1	HRS-07.1_A01
HRS-07.1	HRS-07.1_A02
HRS-07.1	HRS-07.1_A03
HRS-07.1	HRS-07.1_A04
HRS-08	HRS-08_A01
HRS-08	HRS-08_A02
HRS-08	HRS-08_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

HRS-08	HRS-08_A10
HRS-08	HRS-08_A11
HRS-09	HRS-09_A01
HRS-09	HRS-09_A02
HRS-09	HRS-09_A03
HRS-09	HRS-09_A04
HRS-09	HRS-09_A05
HRS-09	HRS-09_A06
HRS-09	HRS-09_A07
HRS-09	HRS-09_A08
HRS-09	HRS-09_A09
HRS-09	HRS-09_A10
HRS-09.1	HRS-09.1_A01
HRS-09.2	HRS-09.2_A01
HRS-09.2	HRS-09.2_A02
HRS-09.2	HRS-09.2_A03
HRS-09.2	HRS-09.2_A04
HRS-09.2	HRS-09.2_A05
HRS-09.2	HRS-09.2_A06
HRS-09.2	HRS-09.2_A07
HRS-09.3	HRS-09.3_A01
HRS-09.3	HRS-09.3_A02
HRS-09.4	HRS-09.4_A01
HRS-09.4	HRS-09.4_A02
HRS-09.4	HRS-09.4_A03
HRS-10	HRS-10_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

HRS-11	HRS-11_A01
HRS-11	HRS-11_A02
HRS-11	HRS-11_A03
HRS-12	HRS-12_A01
HRS-12.1	HRS-12.1_A01
HRS-12.1	HRS-12.1_A02
HRS-12.1	HRS-12.1_A03
HRS-12.1	HRS-12.1_A04
HRS-13	HRS-13_A01
HRS-13	HRS-13_A02
HRS-13.1	HRS-13.1_A01
HRS-13.1	HRS-13.1_A02
HRS-13.2	HRS-13.2_A01
HRS-13.3	HRS-13.3_A01
HRS-13.3	HRS-13.3_A02
HRS-13.4	HRS-13.4_A01
IAC-01	IAC-01_A01
IAC-01.1	IAC-01.1_A01
IAC-01.1	IAC-01.1_A02
IAC-01.1	IAC-01.1_A03
IAC-01.1	IAC-01.1_A04
IAC-02	IAC-02_A01
IAC-02	IAC-02_A02
IAC-02	IAC-02_A03
IAC-02	IAC-02_A04
IAC-02	IAC-02_A05

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-02.2	IAC-02.2_A04
IAC-02.2	IAC-02.2_A05
IAC-02.3	IAC-02.3_A01
IAC-02.3	IAC-02.3_A02
IAC-02.3	IAC-02.3_A03
IAC-02.3	IAC-02.3_A04
IAC-02.4	IAC-02.4_A01
IAC-02.4	IAC-02.4_A02
IAC-02.4	IAC-02.4_A03
IAC-03	IAC-03_A01
IAC-03.1	IAC-03.1_A01
IAC-03.1	IAC-03.1_A02
IAC-03.2	IAC-03.2_A01
IAC-03.2	IAC-03.2_A02
IAC-03.2	IAC-03.2_A03
IAC-03.3	IAC-03.3_A01
IAC-03.3	IAC-03.3_A02
IAC-03.4	IAC-03.4_A01
IAC-03.4	IAC-03.4_A02
IAC-03.5	IAC-03.5_A01
IAC-04	IAC-04_A01
IAC-04	IAC-04_A02
IAC-04	IAC-04_A03
IAC-04	IAC-04_A04
IAC-04	IAC-04_A05
IAC-04	IAC-04_A06

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-05.1	IAC-05.1_A01
IAC-05.2	IAC-05.2_A01
IAC-06	IAC-06_A01
IAC-06	IAC-06_A02
IAC-06	IAC-06_A03
IAC-06	IAC-06_A04
IAC-06	IAC-06_A05
IAC-06.1	IAC-06.1_A01
IAC-06.1	IAC-06.1_A02
IAC-06.2	IAC-06.2_A01
IAC-06.3	IAC-06.3_A01
IAC-06.3	IAC-06.3_A02
IAC-06.4	IAC-06.4_A01
IAC-06.4	IAC-06.4_A02
IAC-07	IAC-07_A01
IAC-07.1	IAC-07.1_A01
IAC-07.2	IAC-07.2_A01
IAC-07.2	IAC-07.2_A02
IAC-07.2	IAC-07.2_A03
IAC-07.2	IAC-07.2_A04
IAC-07.2	IAC-07.2_A05
IAC-07.2	IAC-07.2_A06
IAC-07.2	IAC-07.2_A07
IAC-07.2	IAC-07.2_A08
IAC-07.2	IAC-07.2_A09
IAC-07.2	IAC-07.2_A10

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-07.2	IAC-07.2_A17
IAC-07.2	IAC-07.2_A18
IAC-07.2	IAC-07.2_A19
IAC-07.2	IAC-07.2_A20
IAC-07.2	IAC-07.2_A21
IAC-07.2	IAC-07.2_A22
IAC-07.2	IAC-07.2_A23
IAC-07.2	IAC-07.2_A24
IAC-07.2	IAC-07.2_A25
IAC-07.2	IAC-07.2_A26
IAC-07.2	IAC-07.2_A27
IAC-07.2	IAC-07.2_A28
IAC-07.2	IAC-07.2_A29
IAC-07.2	IAC-07.2_A30
IAC-07.2	IAC-07.2_A31
IAC-07.2	IAC-07.2_A32
IAC-07.2	IAC-07.2_A33
IAC-07.2	IAC-07.2_A34
IAC-07.2	IAC-07.2_A35
IAC-07.2	IAC-07.2_A36
IAC-07.2	IAC-07.2_A37
IAC-07.2	IAC-07.2_A38
IAC-07.2	IAC-07.2_A39
IAC-07.2	IAC-07.2_A40
IAC-08	IAC-08_A01
IAC-08	IAC-08_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-09	IAC-09_A01
IAC-09	IAC-09_A02
IAC-09	IAC-09_A03
IAC-09	IAC-09_A04
IAC-09	IAC-09_A05
IAC-09	IAC-09_A06
IAC-09.1	IAC-09.1_A01
IAC-09.1	IAC-09.1_A02
IAC-09.2	IAC-09.2_A01
IAC-09.2	IAC-09.2_A02
IAC-09.3	IAC-09.3_A01
IAC-09.3	IAC-09.3_A02
IAC-09.3	IAC-09.3_A03
IAC-09.4	IAC-09.4_A01
IAC-09.4	IAC-09.4_A02
IAC-09.5	IAC-09.5_A01
IAC-09.5	IAC-09.5_A02
IAC-09.6	IAC-09.6_A01
IAC-10	IAC-10_A01
IAC-10	IAC-10_A02
IAC-10	IAC-10_A03
IAC-10	IAC-10_A04
IAC-10	IAC-10_A05
IAC-10	IAC-10_A06
IAC-10	IAC-10_A07
IAC-10	IAC-10_A08

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-10	IAC-10_A15
IAC-10	IAC-10_A16
IAC-10	IAC-10_A17
IAC-10.1	IAC-10.1_A01
IAC-10.1	IAC-10.1_A02
IAC-10.1	IAC-10.1_A03
IAC-10.1	IAC-10.1_A04
IAC-10.1	IAC-10.1_A05
IAC-10.1	IAC-10.1_A06
IAC-10.1	IAC-10.1_A07
IAC-10.1	IAC-10.1_A08
IAC-10.1	IAC-10.1_A09
IAC-10.1	IAC-10.1_A10
IAC-10.1	IAC-10.1_A11
IAC-10.1	IAC-10.1_A12
IAC-10.2	IAC-10.2_A01
IAC-10.2	IAC-10.2_A02
IAC-10.2	IAC-10.2_A03
IAC-10.2	IAC-10.2_A04
IAC-10.3	IAC-10.3_A01
IAC-10.4	IAC-10.4_A01
IAC-10.4	IAC-10.4_A02
IAC-10.4	IAC-10.4_A03
IAC-10.4	IAC-10.4_A04
IAC-10.5	IAC-10.5_A01
IAC-10.5	IAC-10.5_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-10.10	IAC-10.10_A01
IAC-10.10	IAC-10.10_A02
IAC-10.11	IAC-10.11_A01
IAC-10.11	IAC-10.11_A02
IAC-10.11	IAC-10.11_A03
IAC-10.11	IAC-10.11_A04
IAC-10.11	IAC-10.11_A05
IAC-10.11	IAC-10.11_A06
IAC-10.11	IAC-10.11_A07
IAC-10.12	IAC-10.12_A01
IAC-10.12	IAC-10.12_A02
IAC-11	IAC-11_A01
IAC-11	IAC-11_A02
IAC-12	IAC-12_A01
IAC-12.1	IAC-12.1_A01
IAC-13	IAC-13_A01
IAC-13	IAC-13_A02
IAC-13	IAC-13_A03
IAC-13.1	IAC-13.1_A01
IAC-13.1	IAC-13.1_A02
IAC-13.2	IAC-13.2_A01
IAC-13.2	IAC-13.2_A02
IAC-14	IAC-14_A01
IAC-14	IAC-14_A02
IAC-15	IAC-15_A01
IAC-15	IAC-15_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-15	IAC-15_A09
IAC-15	IAC-15_A10
IAC-15	IAC-15_A11
IAC-15	IAC-15_A12
IAC-15	IAC-15_A13
IAC-15	IAC-15_A14
IAC-15	IAC-15_A15
IAC-15	IAC-15_A16
IAC-15	IAC-15_A17
IAC-15	IAC-15_A18
IAC-15	IAC-15_A19
IAC-15	IAC-15_A20
IAC-15	IAC-15_A21
IAC-15	IAC-15_A22
IAC-15	IAC-15_A23
IAC-15	IAC-15_A24
IAC-15	IAC-15_A25
IAC-15	IAC-15_A26
IAC-15	IAC-15_A27
IAC-15	IAC-15_A28
IAC-15	IAC-15_A29
IAC-15	IAC-15_A30
IAC-15	IAC-15_A31
IAC-15	IAC-15_A32
IAC-15	IAC-15_A33
IAC-15	IAC-15_A34

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-15.2	IAC-15.2_A01
IAC-15.2	IAC-15.2_A02
IAC-15.3	IAC-15.3_A01
IAC-15.3	IAC-15.3_A02
IAC-15.3	IAC-15.3_A03
IAC-15.3	IAC-15.3_A04
IAC-15.3	IAC-15.3_A05
IAC-15.3	IAC-15.3_A06
IAC-15.3	IAC-15.3_A07
IAC-15.3	IAC-15.3_A08
IAC-15.4	IAC-15.4_A01
IAC-15.4	IAC-15.4_A02
IAC-15.4	IAC-15.4_A03
IAC-15.4	IAC-15.4_A04
IAC-15.4	IAC-15.4_A05
IAC-15.5	IAC-15.5_A01
IAC-15.5	IAC-15.5_A02
IAC-15.6	IAC-15.6_A01
IAC-15.6	IAC-15.6_A02
IAC-15.6	IAC-15.6_A03
IAC-15.7	IAC-15.7_A01
IAC-15.7	IAC-15.7_A02
IAC-15.8	IAC-15.8_A01
IAC-15.8	IAC-15.8_A02
IAC-15.8	IAC-15.8_A03
IAC-15.9	IAC-15.9_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-17	IAC-17_A01
IAC-17	IAC-17_A02
IAC-17	IAC-17_A03
IAC-17	IAC-17_A04
IAC-18	IAC-18_A01
IAC-19	IAC-19_A01
IAC-20	IAC-20_A01
IAC-20	IAC-20_A02
IAC-20	IAC-20_A03
IAC-20	IAC-20_A04
IAC-20	IAC-20_A05
IAC-20	IAC-20_A06
IAC-20	IAC-20_A07
IAC-20	IAC-20_A08
IAC-20	IAC-20_A09
IAC-20	IAC-20_A10
IAC-20	IAC-20_A11
IAC-20.1	IAC-20.1_A01
IAC-20.2	IAC-20.2_A01
IAC-20.3	IAC-20.3_A01
IAC-20.4	IAC-20.4_A01
IAC-20.5	IAC-20.5_A01
IAC-20.5	IAC-20.5_A02
IAC-20.5	IAC-20.5_A03
IAC-20.5	IAC-20.5_A04
IAC-20.6	IAC-20.6_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-21	IAC-21_A05
IAC-21	IAC-21_A06
IAC-21	IAC-21_A07
IAC-21.1	IAC-21.1_A01
IAC-21.1	IAC-21.1_A02
IAC-21.1	IAC-21.1_A03
IAC-21.1	IAC-21.1_A04
IAC-21.1	IAC-21.1_A05
IAC-21.1	IAC-21.1_A06
IAC-21.1	IAC-21.1_A07
IAC-21.1	IAC-21.1_A08
IAC-21.1	IAC-21.1_A09
IAC-21.2	IAC-21.2_A01
IAC-21.2	IAC-21.2_A02
IAC-21.2	IAC-21.2_A03
IAC-21.2	IAC-21.2_A04
IAC-21.3	IAC-21.3_A01
IAC-21.3	IAC-21.3_A02
IAC-21.4	IAC-21.4_A01
IAC-21.5	IAC-21.5_A01
IAC-21.5	IAC-21.5_A02
IAC-21.5	IAC-21.5_A03
IAC-21.5	IAC-21.5_A04
IAC-21.6	IAC-21.6_A01
IAC-21.6	IAC-21.6_A02
IAC-21.6	IAC-21.6_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-22	IAC-22_A04
IAC-22	IAC-22_A05
IAC-22	IAC-22_A06
IAC-22	IAC-22_A07
IAC-22	IAC-22_A08
IAC-22	IAC-22_A09
IAC-23	IAC-23_A01
IAC-23	IAC-23_A02
IAC-23	IAC-23_A03
IAC-24	IAC-24_A01
IAC-24	IAC-24_A02
IAC-24	IAC-24_A03
IAC-24	IAC-24_A04
IAC-24	IAC-24_A05
IAC-24	IAC-24_A06
IAC-24	IAC-24_A07
IAC-24	IAC-24_A08
IAC-24.1	IAC-24.1_A01
IAC-25	IAC-25_A01
IAC-25	IAC-25_A02
IAC-25	IAC-25_A03
IAC-25.1	IAC-25.1_A01
IAC-25.1	IAC-25.1_A02
IAC-26	IAC-26_A01
IAC-26	IAC-26_A02
IAC-26	IAC-26_A03_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAC-28	IAC-28_A04
IAC-28	IAC-28_A05
IAC-28.1	IAC-28.1_A01
IAC-28.1	IAC-28.1_A02
IAC-28.1	IAC-28.1_A03
IAC-28.2	IAC-28.2_A01
IAC-28.3	IAC-28.3_A01
IAC-28.3	IAC-28.3_A02
IAC-28.4	IAC-28.4_A01
IAC-28.5	IAC-28.5_A01
IAC-29	IAC-29_A01
IRO-01	IRO-01_A01
IRO-01	IRO-01_A02
IRO-01	IRO-01_A03
IRO-01	IRO-01_A04
IRO-01	IRO-01_A05
IRO-01	IRO-01_A06
IRO-01	IRO-01_A07
IRO-01	IRO-01_A08
IRO-01	IRO-01_A09
IRO-01	IRO-01_A10
IRO-01	IRO-01_A11
IRO-01	IRO-01_A12
IRO-01	IRO-01_A13
IRO-02	IRO-02_A01
IRO-02	IRO-02_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IRO-02	IRO-02_A09
IRO-02	IRO-02_A10
IRO-02	IRO-02_A11
IRO-02	IRO-02_A12
IRO-02	IRO-02_A13
IRO-02	IRO-02_A14
IRO-02	IRO-02_A15
IRO-02	IRO-02_A16
IRO-02	IRO-02_A17
IRO-02	IRO-02_A18
IRO-02	IRO-02_A19
IRO-02	IRO-02_A20
IRO-02.1	IRO-02.1_A01
IRO-02.1	IRO-02.1_A02
IRO-02.1	IRO-02.1_A03
IRO-02.1	IRO-02.1_A04
IRO-02.1	IRO-02.1_A05
IRO-02.1	IRO-02.1_A06
IRO-02.1	IRO-02.1_A07
IRO-02.1	IRO-02.1_A08
IRO-02.2	IRO-02.2_A01
IRO-02.3	IRO-02.3_A01
IRO-02.3	IRO-02.3_A02
IRO-02.3	IRO-02.3_A03
IRO-02.4	IRO-02.4_A01
IRO-02.4	IRO-02.4_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IRO-03	IRO-03_A01
IRO-03	IRO-03_A02
IRO-03	IRO-03_A03
IRO-03	IRO-03_A04
IRO-04	IRO-04_A01
IRO-04	IRO-04_A02
IRO-04	IRO-04_A03
IRO-04	IRO-04_A04
IRO-04	IRO-04_A05
IRO-04	IRO-04_A06
IRO-04	IRO-04_A07
IRO-04	IRO-04_A08
IRO-04	IRO-04_A09
IRO-04	IRO-04_A10
IRO-04	IRO-04_A11
IRO-04	IRO-04_A12
IRO-04	IRO-04_A13
IRO-04	IRO-04_A14
IRO-04	IRO-04_A15
IRO-04	IRO-04_A16
IRO-04	IRO-04_A17
IRO-04	IRO-04_A18
IRO-04	IRO-04_A19
IRO-04	IRO-04_A20
IRO-04	IRO-04_A21
IRO-04	IRO-04_A22

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IRO-04.2	IRO-04.2_A02
IRO-04.2	IRO-04.2_A03
IRO-04.2	IRO-04.2_A04
IRO-04.2	IRO-04.2_A05
IRO-04.2	IRO-04.2_A06
IRO-04.2	IRO-04.2_A07
IRO-04.2	IRO-04.2_A08
IRO-04.2	IRO-04.2_A09
IRO-04.2	IRO-04.2_A10
IRO-04.2	IRO-04.2_A11
IRO-04.2	IRO-04.2_A12
IRO-04.2	IRO-04.2_A13
IRO-04.2	IRO-04.2_A14
IRO-04.2	IRO-04.2_A15
IRO-04.2	IRO-04.2_A16
IRO-04.2	IRO-04.2_A17
IRO-04.2	IRO-04.2_A18
IRO-04.2	IRO-04.2_A19
IRO-04.2	IRO-04.2_A20
IRO-04.2	IRO-04.2_A21
IRO-04.2	IRO-04.2_A22
IRO-04.2	IRO-04.2_A23
IRO-04.2	IRO-04.2_A24
IRO-04.3	IRO-04.3_A01
IRO-04.3	IRO-04.3_A02
IRO-04.3	IRO-04.3_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IRO-04.3	IRO-04.3_A10
IRO-05	IRO-05_A01
IRO-05	IRO-05_A02
IRO-05	IRO-05_A03
IRO-05	IRO-05_A04
IRO-05	IRO-05_A05
IRO-05	IRO-05_A06
IRO-05	IRO-05_A07
IRO-05	IRO-05_A08
IRO-05	IRO-05_A09
IRO-05	IRO-05_A10
IRO-05	IRO-05_A11
IRO-05.1	IRO-05.1_A01
IRO-05.2	IRO-05.2_A01
IRO-05.2	IRO-05.2_A02
IRO-06	IRO-06_A01
IRO-06	IRO-06_A02
IRO-06	IRO-06_A03
IRO-06	IRO-06_A04
IRO-06	IRO-06_A05
IRO-06	IRO-06_A06
IRO-06.1	IRO-06.1_A01
IRO-07	IRO-07_A01
IRO-07	IRO-07_A02
IRO-07	IRO-07_A03
IRO-08	IRO-08_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IRO-09.1	IRO-09.1_A05
IRO-09.1	IRO-09.1_A06
IRO-10	IRO-10_A01
IRO-10	IRO-10_A02
IRO-10	IRO-10_A03
IRO-10	IRO-10_A04
IRO-10.1	IRO-10.1_A01
IRO-10.1	IRO-10.1_A02
IRO-10.2	IRO-10.2_A01
IRO-10.3	IRO-10.3_A01
IRO-10.3	IRO-10.3_A02
IRO-10.4	IRO-10.4_A01
IRO-10.4	IRO-10.4_A02
IRO-11	IRO-11_A01
IRO-11	IRO-11_A02
IRO-11	IRO-11_A03
IRO-11	IRO-11_A04
IRO-11	IRO-11_A05
IRO-11	IRO-11_A06
IRO-11.1	IRO-11.1_A01
IRO-11.1	IRO-11.1_A02
IRO-11.2	IRO-11.2_A01
IRO-11.2	IRO-11.2_A02
IRO-12	IRO-12_A01
IRO-12	IRO-12_A02
IRO-12	IRO-12_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IRO-12.1	IRO-12.1_A03
IRO-12.2	IRO-12.2_A01
IRO-12.2	IRO-12.2_A02
IRO-12.3	IRO-12.3_A01
IRO-12.3	IRO-12.3_A02
IRO-12.4	IRO-12.4_A01
IRO-12.4	IRO-12.4_A02
IRO-13	IRO-13_A08
IRO-13	IRO-13_A09
IRO-14	IRO-14_A01
IRO-14	IRO-14_A02
IRO-14	IRO-14_A03
IRO-14	IRO-14_A04
IRO-15	IRO-15_A01
IRO-15	IRO-15_A02
IRO-16	IRO-16_A01
IRO-16	IRO-16_A02
IAO-01	IAO-01_A01
IAO-01	IAO-01_A02
IAO-01	IAO-01_A03
IAO-01	IAO-01_A04
IAO-01	IAO-01_A05
IAO-01	IAO-01_A06
IAO-01	IAO-01_A07
IAO-01	IAO-01_A08
IAO-01.1	IAO-01.1_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAO-02	IAO-02_A06
IAO-02	IAO-02_A07
IAO-02	IAO-02_A08
IAO-02	IAO-02_A09
IAO-02	IAO-02_A10
IAO-02	IAO-02_A11
IAO-02	IAO-02_A12
IAO-02	IAO-02_A13
IAO-02	IAO-02_A14
IAO-02	IAO-02_A15
IAO-02	IAO-02_A16
IAO-02	IAO-02_A17
IAO-02	IAO-02_A18
IAO-02	IAO-02_A19
IAO-02	IAO-02_A20
IAO-02.1	IAO-02.1_A01
IAO-02.2	IAO-02.2_A01
IAO-02.2	IAO-02.2_A02
IAO-02.2	IAO-02.2_A03
IAO-02.3	IAO-02.3_A01
IAO-02.3	IAO-02.3_A02
IAO-02.3	IAO-02.3_A03
IAO-02.3	IAO-02.3_A04
IAO-02.4	IAO-02.4_A01
IAO-03	IAO-03_A01
IAO-03	IAO-03_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAO-03	IAO-03_A09
IAO-03	IAO-03_A10
IAO-03	IAO-03_A11
IAO-03	IAO-03_A12
IAO-03	IAO-03_A13
IAO-03	IAO-03_A14
IAO-03	IAO-03_A15
IAO-03	IAO-03_A16
IAO-03	IAO-03_A17
IAO-03	IAO-03_A18
IAO-03	IAO-03_A19
IAO-03	IAO-03_A20
IAO-03	IAO-03_A21
IAO-03	IAO-03_A22
IAO-03	IAO-03_A23
IAO-03	IAO-03_A24
IAO-03	IAO-03_A25
IAO-03	IAO-03_A26
IAO-03	IAO-03_A27
IAO-03	IAO-03_A28
IAO-03	IAO-03_A29
IAO-03	IAO-03_A30
IAO-03	IAO-03_A31
IAO-03	IAO-03_A32
IAO-03	IAO-03_A33
IAO-03	IAO-03_A34

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAO-03	IAO-03_A41
IAO-03	IAO-03_A42
IAO-03	IAO-03_A43
IAO-03	IAO-03_A44
IAO-03	IAO-03_A45
IAO-03	IAO-03_A46
IAO-03	IAO-03_A47
IAO-03	IAO-03_A48
IAO-03	IAO-03_A49
IAO-03.1	IAO-03.1_A01
IAO-03.1	IAO-03.1_A02
IAO-03.2	IAO-03.2_A01
IAO-04	IAO-04_A01
IAO-04	IAO-04_A02
IAO-04	IAO-04_A03
IAO-04	IAO-04_A04
IAO-04	IAO-04_A05
IAO-04	IAO-04_A06
IAO-05	IAO-05_A01
IAO-05	IAO-05_A02
IAO-05	IAO-05_A03
IAO-05	IAO-05_A04
IAO-05	IAO-05_A05
IAO-05	IAO-05_A06
IAO-05	IAO-05_A07
IAO-05	IAO-05_A08

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAO-05	IAO-05_A15
IAO-05	IAO-05_A16
IAO-05	IAO-05_A17
IAO-05	IAO-05_A18
IAO-05	IAO-05_A19
IAO-05	IAO-05_A20
IAO-05	IAO-05_A21
IAO-05	IAO-05_A22
IAO-05	IAO-05_A23
IAO-05.1	IAO-05.1_A01
IAO-05.1	IAO-05.1_A02
IAO-06	IAO-06_A01
IAO-06	IAO-06_A02
IAO-06	IAO-06_A03
IAO-06	IAO-06_A04
IAO-06	IAO-06_A05
IAO-06	IAO-06_A06
IAO-06	IAO-06_A07
IAO-06	IAO-06_A08
IAO-06	IAO-06_A09
IAO-06	IAO-06_A10
IAO-06	IAO-06_A11
IAO-06	IAO-06_A12
IAO-06	IAO-06_A13
IAO-06	IAO-06_A14
IAO-06	IAO-06_A15

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

IAO-07	IAO-07_A03
IAO-07	IAO-07_A04
IAO-07	IAO-07_A05
IAO-07	IAO-07_A06
IAO-07	IAO-07_A07
MNT-01	MNT-01_A01
MNT-01	MNT-01_A02
MNT-01	MNT-01_A03
MNT-01	MNT-01_A04
MNT-01	MNT-01_A05
MNT-01	MNT-01_A06
MNT-01	MNT-01_A07
MNT-01	MNT-01_A08
MNT-01	MNT-01_A09
MNT-01	MNT-01_A10
MNT-01	MNT-01_A11
MNT-01	MNT-01_A12
MNT-01	MNT-01_A13
MNT-01	MNT-01_A14
MNT-01	MNT-01_A15
MNT-01	MNT-01_A16
MNT-01	MNT-01_A17
MNT-01	MNT-01_A18
MNT-01	MNT-01_A19
MNT-01	MNT-01_A20
MNT-01	MNT-01_A21

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MNT-02	MNT-02_A03
MNT-02	MNT-02_A04
MNT-02	MNT-02_A05
MNT-02	MNT-02_A06
MNT-02	MNT-02_A07
MNT-02	MNT-02_A08
MNT-02	MNT-02_A09
MNT-02	MNT-02_A10
MNT-02	MNT-02_A11
MNT-02	MNT-02_A12
MNT-02	MNT-02_A13
MNT-02.1	MNT-02.1_A01
MNT-02.1	MNT-02.1_A02
MNT-02.1	MNT-02.1_A03
MNT-02.1	MNT-02.1_A04
MNT-02.1	MNT-02.1_A05
MNT-02.1	MNT-02.1_A06
MNT-02.1	MNT-02.1_A07
MNT-02.1	MNT-02.1_A08
MNT-02.1	MNT-02.1_A09
MNT-03	MNT-03_A01
MNT-03	MNT-03_A02
MNT-03	MNT-03_A03
MNT-03.1	MNT-03.1_A01
MNT-03.1	MNT-03.1_A02
MNT-03.1	MNT-03.1_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MNT-04	MNT-04_A02
MNT-04	MNT-04_A03
MNT-04	MNT-04_A04
MNT-04	MNT-04_A05
MNT-04	MNT-04_A06
MNT-04	MNT-04_A07
MNT-04	MNT-04_A08
MNT-04	MNT-04_A09
MNT-04	MNT-04_A10
MNT-04.1	MNT-04.1_A01
MNT-04.2	MNT-04.2_A01
MNT-04.3	MNT-04.3_A01
MNT-04.3	MNT-04.3_A02
MNT-04.3	MNT-04.3_A03
MNT-04.3	MNT-04.3_A04
MNT-04.3	MNT-04.3_A05
MNT-04.4	MNT-04.4_A01
MNT-05	MNT-05_A01
MNT-05	MNT-05_A02
MNT-05	MNT-05_A03
MNT-05	MNT-05_A04
MNT-05	MNT-05_A05
MNT-05	MNT-05_A06
MNT-05	MNT-05_A07
MNT-05	MNT-05_A08
MNT-05	MNT-05_A09

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MNT-05.1	MNT-05.1_A06
MNT-05.2	MNT-05.2_A01
MNT-05.3	MNT-05.3_A01
MNT-05.3	MNT-05.3_A02
MNT-05.3	MNT-05.3_A03
MNT-05.4	MNT-05.4_A01
MNT-05.4	MNT-05.4_A02
MNT-05.5	MNT-05.5_A01
MNT-05.5	MNT-05.5_A02
MNT-05.5	MNT-05.5_A03
MNT-05.5	MNT-05.5_A04
MNT-05.6	MNT-05.6_A01
MNT-05.6	MNT-05.6_A02
MNT-05.6	MNT-05.6_A03
MNT-05.6	MNT-05.6_A04
MNT-05.6	MNT-05.6_A05
MNT-05.7	MNT-05.7_A01
MNT-05.7	MNT-05.7_A02
MNT-05.7	MNT-05.7_A03
MNT-05.7	MNT-05.7_A04
MNT-06	MNT-06_A01
MNT-06	MNT-06_A02
MNT-06	MNT-06_A03
MNT-06	MNT-06_A04
MNT-06	MNT-06_A05
MNT-06.1	MNT-06.1_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MNT-06.1	MNT-06.1_A08
MNT-06.1	MNT-06.1_A09
MNT-06.1	MNT-06.1_A10
MNT-06.1	MNT-06.1_A11
MNT-06.2	MNT-06.2_A01
MNT-07	MNT-07_A01
MNT-07	MNT-07_A02
MNT-07	MNT-07_A03
MNT-08	MNT-08_A01
MNT-08	MNT-08_A02
MNT-08	MNT-08_A03
MNT-09	MNT-09_A01
MNT-10	MNT-10_A01
MNT-11	MNT-11_A01
MDM-01	MDM-01_A01
MDM-02	MDM-02_A01
MDM-02	MDM-02_A02
MDM-02	MDM-02_A03
MDM-02	MDM-02_A04
MDM-02	MDM-02_A05
MDM-02	MDM-02_A06
MDM-03	MDM-03_A01
MDM-03	MDM-03_A02
MDM-03	MDM-03_A03
MDM-03	MDM-03_A04
MDM-04	MDM-04_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

MDM-05	MDM-05_A05
MDM-05	MDM-05_A06
MDM-05	MDM-05_A07
MDM-06	MDM-06_A01
MDM-07	MDM-07_A01
MDM-08	MDM-08_A01
MDM-09	MDM-09_A01
MDM-10	MDM-10_A01
MDM-11	MDM-11_A01
NET-01	NET-01_A01
NET-01	NET-01_A02
NET-01	NET-01_A03
NET-01	NET-01_A04
NET-01	NET-01_A05
NET-01	NET-01_A06
NET-01	NET-01_A07
NET-01	NET-01_A08
NET-01	NET-01_A09
NET-01	NET-01_A10
NET-01	NET-01_A11
NET-01	NET-01_A12
NET-01	NET-01_A13
NET-01	NET-01_A14
NET-01	NET-01_A15
NET-01	NET-01_A16
NET-01	NET-01_A17

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

NET-01	NET-01_A24
NET-01.1	NET-01.1_A01
NET-01.1	NET-01.1_A02
NET-02	NET-02_A01
NET-02.1	NET-02.1_A01
NET-02.1	NET-02.1_A02
NET-02.1	NET-02.1_A03
NET-02.1	NET-02.1_A04
NET-02.1	NET-02.1_A05
NET-02.1	NET-02.1_A06
NET-02.1	NET-02.1_A07
NET-02.1	NET-02.1_A08
NET-02.1	NET-02.1_A09
NET-02.1	NET-02.1_A10
NET-02.1	NET-02.1_A11
NET-02.2	NET-02.2_A01
NET-02.2	NET-02.2_A02
NET-02.3	NET-02.3_A01
NET-03	NET-03_A01
NET-03	NET-03_A02
NET-03	NET-03_A03
NET-03	NET-03_A04
NET-03	NET-03_A05
NET-03	NET-03_A06
NET-03	NET-03_A07
NET-03	NET-03_A08

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

NET-03	NET-03_A15
NET-03	NET-03_A16
NET-03	NET-03_A17
NET-03	NET-03_A18
NET-03	NET-03_A19
NET-03	NET-03_A20
NET-03.1	NET-03.1_A01
NET-03.2	NET-03.2_A01
NET-03.2	NET-03.2_A02
NET-03.2	NET-03.2_A03
NET-03.2	NET-03.2_A04
NET-03.2	NET-03.2_A05
NET-03.2	NET-03.2_A06
NET-03.2	NET-03.2_A07
NET-03.2	NET-03.2_A08
NET-03.2	NET-03.2_A09
NET-03.2	NET-03.2_A10
NET-03.2	NET-03.2_A11
NET-03.2	NET-03.2_A12
NET-03.2	NET-03.2_A13
NET-03.2	NET-03.2_A14
NET-03.3	NET-03.3_A01
NET-03.4	NET-03.4_A01
NET-03.4	NET-03.4_A02
NET-03.4	NET-03.4_A03
NET-03.4	NET-03.4_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

NET-03.6	NET-03.6_A01
NET-03.6	NET-03.6_A02
NET-03.7	NET-03.7_A01
NET-03.7	NET-03.7_A02
NET-03.7	NET-03.7_A03
NET-03.7	NET-03.7_A04
NET-03.7	NET-03.7_A05
NET-03.7	NET-03.7_A06
NET-03.8	NET-03.8_A01
NET-03.8	NET-03.8_A02
NET-03.8	NET-03.8_A03
NET-03.8	NET-03.8_A04
NET-03.8	NET-03.8_A05
NET-03.8	NET-03.8_A06
NET-03.8	NET-03.8_A07
NET-04	NET-04_A01
NET-04	NET-04_A02
NET-04	NET-04_A03
NET-04	NET-04_A04
NET-04	NET-04_A05
NET-04	NET-04_A06
NET-04	NET-04_A07
NET-04	NET-04_A08
NET-04	NET-04_A09
NET-04	NET-04_A10
NET-04	NET-04_A11

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

NET-04.1	NET-04.1_A06
NET-04.2	NET-04.2_A01
NET-04.2	NET-04.2_A02
NET-04.2	NET-04.2_A03
NET-04.2	NET-04.2_A04
NET-04.2	NET-04.2_A05
NET-04.2	NET-04.2_A06
NET-04.2	NET-04.2_A07
NET-04.2	NET-04.2_A08
NET-04.2	NET-04.2_A09
NET-04.2	NET-04.2_A10
NET-04.2	NET-04.2_A11
NET-04.2	NET-04.2_A12
NET-04.2	NET-04.2_A13
NET-04.2	NET-04.2_A14
NET-04.3	NET-04.3_A01
NET-04.3	NET-04.3_A02
NET-04.3	NET-04.3_A03
NET-04.4	NET-04.4_A01
NET-04.4	NET-04.4_A02
NET-04.5	NET-04.5_A01
NET-04.5	NET-04.5_A02
NET-04.5	NET-04.5_A03
NET-04.5	NET-04.5_A04
NET-04.5	NET-04.5_A05
NET-04.6	NET-04.6_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

NET-04.7	NET-04.7_A05
NET-04.7	NET-04.7_A06
NET-04.7	NET-04.7_A07
NET-04.7	NET-04.7_A08
NET-04.7	NET-04.7_A09
NET-04.7	NET-04.7_A10
NET-04.7	NET-04.7_A11
NET-04.7	NET-04.7_A12
NET-04.8	NET-04.8_A01
NET-04.8	NET-04.8_A02
NET-04.9	NET-04.9_A01
NET-04.9	NET-04.9_A02
NET-04.10	NET-04.10_A01
NET-04.10	NET-04.10_A02
NET-04.10	NET-04.10_A03
NET-04.10	NET-04.10_A04
NET-04.10	NET-04.10_A05
NET-04.10	NET-04.10_A06
NET-04.11	NET-04.11_A01
NET-04.11	NET-04.11_A02
NET-04.11	NET-04.11_A03
NET-04.12	NET-04.12_A01
NET-04.13	NET-04.13_A01
NET-04.13	NET-04.13_A02
NET-04.13	NET-04.13_A03
NET-04.13	NET-04.13_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

NET-05	NET-05_A07
NET-05	NET-05_A08
NET-05	NET-05_A09
NET-05	NET-05_A10
NET-05	NET-05_A11
NET-05	NET-05_A12
NET-05	NET-05_A13
NET-05	NET-05_A14
NET-05.1	NET-05.1_A01
NET-05.1	NET-05.1_A02
NET-05.1	NET-05.1_A03
NET-05.2	NET-05.2_A01
NET-05.2	NET-05.2_A02
NET-05.2	NET-05.2_A03
NET-05.2	NET-05.2_A04
NET-05.2	NET-05.2_A05
NET-05.2	NET-05.2_A06
NET-05.2	NET-05.2_A07
NET-05.2	NET-05.2_A08
NET-05.2	NET-05.2_A09
NET-05.2	NET-05.2_A10
NET-06	NET-06_A01
NET-06	NET-06_A02
NET-06	NET-06_A03
NET-06	NET-06_A04
NET-06	NET-06_A05

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

NET-06.1	NET-06.1_A03
NET-06.1	NET-06.1_A04
NET-06.1	NET-06.1_A05
NET-06.1	NET-06.1_A06
NET-06.1	NET-06.1_A07
NET-06.1	NET-06.1_A08
NET-06.2	NET-06.2_A01
NET-06.3	NET-06.3_A01
NET-06.4	NET-06.4_A01
NET-06.5	NET-06.5_A01
NET-07	NET-07_A01
NET-07	NET-07_A02
NET-07	NET-07_A03
NET-08	NET-08_A01
NET-08.1	NET-08.1_A01
NET-08.2	NET-08.2_A01
NET-09	NET-09_A01
NET-09	NET-09_A02
NET-09	NET-09_A03
NET-09.1	NET-09.1_A01
NET-09.2	NET-09.2_A01
NET-09.2	NET-09.2_A02
NET-09.2	NET-09.2_A03
NET-10	NET-10_A01
NET-10	NET-10_A02
NET-10	NET-10_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

NET-10.2	NET-10.2_A03
NET-10.2	NET-10.2_A04
NET-10.3	NET-10.3_A01
NET-10.4	NET-10.4_A01
NET-11	NET-11_A01
NET-11	NET-11_A02
NET-11	NET-11_A03
NET-11	NET-11_A04
NET-11	NET-11_A05
NET-11	NET-11_A06
NET-11	NET-11_A07
NET-11	NET-11_A08
NET-12	NET-12_A01
NET-12.1	NET-12.1_A01
NET-12.1	NET-12.1_A02
NET-12.1	NET-12.1_A03
NET-12.1	NET-12.1_A04
NET-12.1	NET-12.1_A05
NET-12.1	NET-12.1_A06
NET-12.2	NET-12.2_A01
NET-13	NET-13_A01
NET-13	NET-13_A02
NET-13	NET-13_A03
NET-13	NET-13_A04
NET-14	NET-14_A01
NET-14	NET-14_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

NET-14.1	NET-14.1_A04
NET-14.2	NET-14.2_A01
NET-14.2	NET-14.2_A02
NET-14.3	NET-14.3_A01
NET-14.3	NET-14.3_A02
NET-14.4	NET-14.4_A01
NET-14.4	NET-14.4_A02
NET-14.4	NET-14.4_A03
NET-14.4	NET-14.4_A04
NET-14.4	NET-14.4_A05
NET-14.5	NET-14.5_A01
NET-14.5	NET-14.5_A02
NET-14.5	NET-14.5_A03
NET-14.6	NET-14.6_A01
NET-14.7	NET-14.7_A01
NET-14.7	NET-14.7_A02
NET-14.8	NET-14.8_A01
NET-14.8	NET-14.8_A02
NET-15	NET-15_A01
NET-15	NET-15_A02
NET-15	NET-15_A03
NET-15	NET-15_A04
NET-15	NET-15_A05
NET-15.1	NET-15.1_A01
NET-15.1	NET-15.1_A02
NET-15.1	NET-15.1_A05

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

NET-15.5	NET-15.5_A01
NET-15.5	NET-15.5_A02
NET-16	NET-16_A01
NET-16	NET-16_A02
NET-17	NET-17_A01
NET-17	NET-17_A02
NET-17	NET-17_A03
NET-18	NET-18_A01
NET-18.1	NET-18.1_A01
NET-18.1	NET-18.1_A02
NET-18.1	NET-18.1_A03
NET-18.2	NET-18.2_A01
NET-18.2	NET-18.2_A02
NET-18.2	NET-18.2_A03
NET-18.3	NET-18.3_A01
NET-18.3	NET-18.3_A02
PES-01	PES-01_A01
PES-01	PES-01_A02
PES-01	PES-01_A03
PES-01	PES-01_A04
PES-01	PES-01_A30
PES-01	PES-01_A31
PES-01.1	PES-01.1_A01
PES-02	PES-02_A01
PES-02	PES-02_A02
PES-02	PES-02_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PES-02	PES-02_A10
PES-02.1	PES-02.1_A01
PES-02.2	PES-02.2_A01
PES-03	PES-03_A01
PES-03	PES-03_A02
PES-03	PES-03_A03
PES-03	PES-03_A04
PES-03	PES-03_A05
PES-03	PES-03_A06
PES-03	PES-03_A07
PES-03	PES-03_A08
PES-03	PES-03_A09
PES-03	PES-03_A10
PES-03	PES-03_A11
PES-03	PES-03_A12
PES-03	PES-03_A13
PES-03	PES-03_A14
PES-03	PES-03_A15
PES-03	PES-03_A16
PES-03	PES-03_A17
PES-03	PES-03_A18
PES-03	PES-03_A19
PES-03	PES-03_A20
PES-03	PES-03_A21
PES-03	PES-03_A22
PES-03	PES-03_A23

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PES-03.2	PES-03.2_A01
PES-03.2	PES-03.2_A02
PES-03.3	PES-03.3_A01
PES-03.3	PES-03.3_A02
PES-03.3	PES-03.3_A03
PES-03.3	PES-03.3_A04
PES-03.3	PES-03.3_A05
PES-03.3	PES-03.3_A06
PES-03.3	PES-03.3_A07
PES-03.4	PES-03.4_A01
PES-03.4	PES-03.4_A02
PES-03.4	PES-03.4_A03
PES-04	PES-04_A01
PES-04.1	PES-04.1_A01
PES-04.2	PES-04.2_A01
PES-04.3	PES-04.3_A01
PES-05	PES-05_A01
PES-05	PES-05_A02
PES-05	PES-05_A03
PES-05	PES-05_A04
PES-05	PES-05_A05
PES-05	PES-05_A06
PES-05	PES-05_A07
PES-05.1	PES-05.1_A01
PES-05.1	PES-05.1_A02
PES-05.2	PES-05.2_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PES-06.3	PES-06.3_A01
PES-06.3	PES-06.3_A02
PES-06.3	PES-06.3_A03
PES-06.3	PES-06.3_A04
PES-06.4	PES-06.4_A01
PES-06.4	PES-06.4_A02
PES-06.4	PES-06.4_A03
PES-06.4	PES-06.4_A04
PES-06.5	PES-06.5_A01
PES-06.5	PES-06.5_A02
PES-06.5	PES-06.5_A03
PES-06.5	PES-06.5_A04
PES-06.6	PES-06.6_A01
PES-07.7	PES-07.7_A01
PES-07.7	PES-07.7_A02
PES-07	PES-07_A01
PES-07	PES-07_A02
PES-07.1	PES-07.1_A01
PES-07.1	PES-07.1_A02
PES-07.2	PES-07.2_A01
PES-07.2	PES-07.2_A02
PES-07.2	PES-07.2_A03
PES-07.2	PES-07.2_A04
PES-07.2	PES-07.2_A05
PES-07.3	PES-07.3_A01
PES-07.3	PES-07.3_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PES-07.5	PES-07.5_A02
PES-07.5	PES-07.5_A03
PES-07.5	PES-07.5_A04
PES-07.6	PES-07.6_A01
PES-07.6	PES-07.6_A02
PES-07.6	PES-07.6_A03
PES-07.6	PES-07.6_A04
PES-08	PES-08_A01
PES-08	PES-08_A02
PES-08	PES-08_A03
PES-08	PES-08_A04
PES-08	PES-08_A05
PES-08	PES-08_A06
PES-08.1	PES-08.1_A01
PES-08.1	PES-08.1_A02
PES-08.1	PES-08.1_A03
PES-08.1	PES-08.1_A04
PES-08.1	PES-08.1_A05
PES-08.2	PES-08.2_A01
PES-08.2	PES-08.2_A02
PES-08.2	PES-08.2_A03
PES-08.2	PES-08.2_A04
PES-08.2	PES-08.2_A05
PES-08.3	PES-08.3_A01
PES-09	PES-09_A01
PES-09	PES-09_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PES-10	PES-10_A01
PES-10	PES-10_A02
PES-10	PES-10_A03
PES-10	PES-10_A04
PES-10	PES-10_A05
PES-10	PES-10_A06
PES-10	PES-10_A07
PES-11	PES-11_A01
PES-11	PES-11_A02
PES-11	PES-11_A03
PES-11	PES-11_A04
PES-11	PES-11_A05
PES-11	PES-11_A06
PES-11	PES-11_A07
PES-11	PES-11_A08
PES-12	PES-12_A01
PES-12	PES-12_A02
PES-12	PES-12_A03
PES-12	PES-12_A04
PES-12	PES-12_A05
PES-12	PES-12_A06
PES-12.1	PES-12.1_A01
PES-12.1	PES-12.1_A02
PES-12.1	PES-12.1_A03
PES-12.1	PES-12.1_A04
PES-12.1	PES-12.1_A05

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PES-14	PES-14_A04
PES-15	PES-15_A01
PES-15	PES-15_A02
PES-15	PES-15_A03
PES-16	PES-16_A01
PES-16	PES-16_A02
PES-17	PES-17_A01
PES-18	PES-18_A01
PRI-01	PRI-01_A01
PRI-01	PRI-01_A02
PRI-01	PRI-01_A03
PRI-01	PRI-01_A04
PRI-01	PRI-01_A05
PRI-01	PRI-01_A06
PRI-01	PRI-01_A07
PRI-01	PRI-01_A08
PRI-01	PRI-01_A09
PRI-01	PRI-01_A10
PRI-01	PRI-01_A11
PRI-01	PRI-01_A12
PRI-01	PRI-01_A13
PRI-01	PRI-01_A14
PRI-01	PRI-01_A15
PRI-01	PRI-01_A16
PRI-01	PRI-01_A17
PRI-01	PRI-01_A18

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-01.2	PRI-01.2_A01
PRI-01.3	PRI-01.3_A01
PRI-01.3	PRI-01.3_A02
PRI-01.3	PRI-01.3_A03
PRI-01.3	PRI-01.3_A04
PRI-01.3	PRI-01.3_A05
PRI-01.3	PRI-01.3_A06
PRI-01.3	PRI-01.3_A07
PRI-01.4	PRI-01.4_A01
PRI-01.4	PRI-01.4_A02
PRI-01.5	PRI-01.5_A01
PRI-01.6	PRI-01.6_A01
PRI-01.7	PRI-01.7_A01
PRI-02	PRI-02_A01
PRI-02	PRI-02_A02
PRI-02	PRI-02_A03
PRI-02	PRI-02_A04
PRI-02	PRI-02_A05
PRI-02	PRI-02_A06
PRI-02	PRI-02_A07
PRI-02	PRI-02_A08
PRI-02	PRI-02_A09
PRI-02	PRI-02_A10
PRI-02	PRI-02_A11
PRI-02	PRI-02_A12
PRI-02	PRI-02_A13

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-02.1	PRI-02.1_A03
PRI-02.1	PRI-02.1_A04
PRI-02.1	PRI-02.1_A05
PRI-02.1	PRI-02.1_A06
PRI-02.1	PRI-02.1_A07
PRI-02.1	PRI-02.1_A08
PRI-02.1	PRI-02.1_A09
PRI-02.1	PRI-02.1_A10
PRI-02.2	PRI-02.2_A01
PRI-02.2	PRI-02.2_A02
PRI-02.3	PRI-02.3_A01
PRI-02.3	PRI-02.3_A02
PRI-02.3	PRI-02.3_A03
PRI-02.3	PRI-02.3_A04
PRI-02.3	PRI-02.3_A05
PRI-02.3	PRI-02.3_A06
PRI-02.3	PRI-02.3_A07
PRI-02.4	PRI-02.4_A01
PRI-02.4	PRI-02.4_A02
PRI-02.4	PRI-02.4_A03
PRI-02.4	PRI-02.4_A04
PRI-02.5	PRI-02.5_A01
PRI-02.5	PRI-02.5_A02
PRI-02.6	PRI-02.6_A01
PRI-02.6	PRI-02.6_A02
PRI-02.6	PRI-02.6_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-03.2	PRI-03.2_A01
PRI-03.2	PRI-03.2_A02
PRI-03.2	PRI-03.2_A03
PRI-03.2	PRI-03.2_A04
PRI-03.3	PRI-03.3_A01
PRI-03.3	PRI-03.3_A02
PRI-03.4	PRI-03.4_A01
PRI-03.4	PRI-03.4_A02
PRI-03.5	PRI-03.5_A01
PRI-03.6	PRI-03.6_A01
PRI-03.7	PRI-03.7_A01
PRI-03.8	PRI-03.8_A01
PRI-04	PRI-04_A01
PRI-04	PRI-04_A02
PRI-04.1	PRI-04.1_A01
PRI-04.1	PRI-04.1_A02
PRI-04.1	PRI-04.1_A03
PRI-04.2	PRI-04.2_A01
PRI-04.3	PRI-04.3_A01
PRI-04.3	PRI-04.3_A02
PRI-04.4	PRI-04.4_A01
PRI-04.5	PRI-04.5_A01
PRI-04.6	PRI-04.6_A01
PRI-05	PRI-05_A01
PRI-05	PRI-05_A02
PRI-05	PRI-05_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-05	PRI-05_A10
PRI-05.1	PRI-05.1_A01
PRI-05.1	PRI-05.1_A02
PRI-05.1	PRI-05.1_A03
PRI-05.1	PRI-05.1_A04
PRI-05.1	PRI-05.1_A05
PRI-05.1	PRI-05.1_A06
PRI-05.1	PRI-05.1_A07
PRI-05.1	PRI-05.1_A08
PRI-05.1	PRI-05.1_A09
PRI-05.1	PRI-05.1_A10
PRI-05.1	PRI-05.1_A11
PRI-05.1	PRI-05.1_A12
PRI-05.1	PRI-05.1_A13
PRI-05.1	PRI-05.1_A14
PRI-05.1	PRI-05.1_A15
PRI-05.1	PRI-05.1_A16
PRI-05.1	PRI-05.1_A17
PRI-05.1	PRI-05.1_A18
PRI-05.1	PRI-05.1_A19
PRI-05.1	PRI-05.1_A20
PRI-05.1	PRI-05.1_A21
PRI-05.1	PRI-05.1_A22
PRI-05.1	PRI-05.1_A23
PRI-05.1	PRI-05.1_A24
PRI-05.1	PRI-05.1_A25

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-05.1	PRI-05.1_A32
PRI-05.1	PRI-05.1_A33
PRI-05.1	PRI-05.1_A34
PRI-05.1	PRI-05.1_A35
PRI-05.1	PRI-05.1_A36
PRI-05.1	PRI-05.1_A37
PRI-05.1	PRI-05.1_A38
PRI-05.1	PRI-05.1_A39
PRI-05.1	PRI-05.1_A40
PRI-05.1	PRI-05.1_A41
PRI-05.1	PRI-05.1_A42
PRI-05.1	PRI-05.1_A43
PRI-05.1	PRI-05.1_A44
PRI-05.1	PRI-05.1_A45
PRI-05.1	PRI-05.1_A46
PRI-05.1	PRI-05.1_A47
PRI-05.1	PRI-05.1_A48
PRI-05.1	PRI-05.1_A49
PRI-05.2	PRI-05.2_A01
PRI-05.2	PRI-05.2_A02
PRI-05.2	PRI-05.2_A03
PRI-05.3	PRI-05.3_A01
PRI-05.4	PRI-05.4_A01
PRI-05.4	PRI-05.4_A02
PRI-05.4	PRI-05.4_A03
PRI-05.4	PRI-05.4_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-05.4	PRI-05.4_A11
PRI-05.4	PRI-05.4_A12
PRI-05.4	PRI-05.4_A13
PRI-05.4	PRI-05.4_A14
PRI-05.4	PRI-05.4_A15
PRI-05.4	PRI-05.4_A16
PRI-05.4	PRI-05.4_A17
PRI-05.4	PRI-05.4_A18
PRI-05.4	PRI-05.4_A19
PRI-05.4	PRI-05.4_A20
PRI-05.4	PRI-05.4_A21
PRI-05.4	PRI-05.4_A22
PRI-05.4	PRI-05.4_A23
PRI-05.4	PRI-05.4_A24
PRI-05.4	PRI-05.4_A25
PRI-05.4	PRI-05.4_A26
PRI-05.4	PRI-05.4_A27
PRI-05.4	PRI-05.4_A28
PRI-05.4	PRI-05.4_A29
PRI-05.4	PRI-05.4_A30
PRI-05.4	PRI-05.4_A31
PRI-05.4	PRI-05.4_A32
PRI-05.4	PRI-05.4_A33
PRI-05.4	PRI-05.4_A34
PRI-05.4	PRI-05.4_A35
PRI-05.4	PRI-05.4_A36

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-05.6	PRI-05.6_A03
PRI-05.6	PRI-05.6_A04
PRI-05.7	PRI-05.7_A01
PRI-05.7	PRI-05.7_A02
PRI-05.7	PRI-05.7_A03
PRI-05.7	PRI-05.7_A04
PRI-05.7	PRI-05.7_A05
PRI-05.7	PRI-05.7_A06
PRI-05.7	PRI-05.7_A07
PRI-05.7	PRI-05.7_A08
PRI-05.7	PRI-05.7_A09
PRI-06	PRI-06_A01
PRI-06	PRI-06_A02
PRI-06	PRI-06_A03
PRI-06	PRI-06_A04
PRI-06.1	PRI-06.1_A01
PRI-06.1	PRI-06.1_A02
PRI-06.2	PRI-06.2_A01
PRI-06.2	PRI-06.2_A02
PRI-06.3	PRI-06.3_A01
PRI-06.3	PRI-06.3_A02
PRI-06.3	PRI-06.3_A03
PRI-06.3	PRI-06.3_A04
PRI-06.3	PRI-06.3_A05
PRI-06.3	PRI-06.3_A06
PRI-06.3	PRI-06.3_A07

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-06.4	PRI-06.4_A01
PRI-06.4	PRI-06.4_A02
PRI-06.4	PRI-06.4_A03
PRI-06.4	PRI-06.4_A04
PRI-06.4	PRI-06.4_A05
PRI-06.4	PRI-06.4_A06
PRI-06.4	PRI-06.4_A07
PRI-06.4	PRI-06.4_A08
PRI-06.4	PRI-06.4_A09
PRI-06.4	PRI-06.4_A10
PRI-06.4	PRI-06.4_A11
PRI-06.4	PRI-06.4_A12
PRI-06.4	PRI-06.4_A13
PRI-06.5	PRI-06.5_A01
PRI-06.5	PRI-06.5_A02
PRI-06.6	PRI-06.6_A01
PRI-06.7	PRI-06.7_A01
PRI-07	PRI-07_A01
PRI-07	PRI-07_A02
PRI-07	PRI-07_A03
PRI-07	PRI-07_A04
PRI-07.1	PRI-07.1_A01
PRI-07.2	PRI-07.2_A01
PRI-07.3	PRI-07.3_A01
PRI-07.4	PRI-07.4_A01
PRI-08	PRI-08_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-08	PRI-08_A08
PRI-08	PRI-08_A09
PRI-08	PRI-08_A10
PRI-08	PRI-08_A11
PRI-08	PRI-08_A12
PRI-09	PRI-09_A01
PRI-09	PRI-09_A02
PRI-09	PRI-09_A03
PRI-09	PRI-09_A04
PRI-10	PRI-10_A01
PRI-10	PRI-10_A02
PRI-10	PRI-10_A03
PRI-10	PRI-10_A04
PRI-10	PRI-10_A05
PRI-10	PRI-10_A06
PRI-10	PRI-10_A07
PRI-10	PRI-10_A08
PRI-10	PRI-10_A09
PRI-10	PRI-10_A10
PRI-10	PRI-10_A11
PRI-10	PRI-10_A12
PRI-10	PRI-10_A13
PRI-10	PRI-10_A14
PRI-10	PRI-10_A15
PRI-10	PRI-10_A16
PRI-10	PRI-10_A17

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-10.1	PRI-10.1_A02
PRI-10.2	PRI-10.2_A01
PRI-10.2	PRI-10.2_A02
PRI-11	PRI-11_A01
PRI-11	PRI-11_A02
PRI-11	PRI-11_A03
PRI-12	PRI-12_A01
PRI-12	PRI-12_A02
PRI-13	PRI-13_A01
PRI-13	PRI-13_A02
PRI-13	PRI-13_A03
PRI-13	PRI-13_A04
PRI-13	PRI-13_A05
PRI-13	PRI-13_A06
PRI-14	PRI-14_A01
PRI-14	PRI-14_A02
PRI-14	PRI-14_A03
PRI-14	PRI-14_A04
PRI-14	PRI-14_A05
PRI-14	PRI-14_A06
PRI-14	PRI-14_A07
PRI-14	PRI-14_A08
PRI-14	PRI-14_A09
PRI-14.1	PRI-14.1_A01
PRI-14.1	PRI-14.1_A02
PRI-14.1	PRI-14.1_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRI-15	PRI-15_A01
PRI-15	PRI-15_A02
PRI-16	PRI-16_A01
PRI-16	PRI-16_A02
PRI-16	PRI-16_A03
PRI-16	PRI-16_A04
PRI-17	PRI-17_A01
PRI-17	PRI-17_A02
PRI-17.1	PRI-17.1_A01
PRI-17.1	PRI-17.1_A02
PRI-17.2	PRI-17.2_A01
PRM-01	PRM-01_A01
PRM-01	PRM-01_A02
PRM-01	PRM-01_A03
PRM-01	PRM-01_A04
PRM-01	PRM-01_A05
PRM-01	PRM-01_A06
PRM-01	PRM-01_A07
PRM-01	PRM-01_A08
PRM-01	PRM-01_A09
PRM-01	PRM-01_A10
PRM-01	PRM-01_A11
PRM-01	PRM-01_A12
PRM-01	PRM-01_A13
PRM-01	PRM-01_A14
PRM-01	PRM-01_A15

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRM-01	PRM-01_A22
PRM-01	PRM-01_A23
PRM-01	PRM-01_A24
PRM-01	PRM-01_A25
PRM-01.1	PRM-01.1_A01
PRM-01.1	PRM-01.1_A02
PRM-01.2	PRM-01.2_A01
PRM-01.2	PRM-01.2_A02
PRM-02	PRM-02_A01
PRM-02	PRM-02_A02
PRM-02	PRM-02_A03
PRM-02	PRM-02_A04
PRM-02	PRM-02_A05
PRM-02	PRM-02_A06
PRM-03	PRM-03_A01
PRM-03	PRM-03_A02
PRM-03	PRM-03_A03
PRM-03	PRM-03_A04
PRM-03	PRM-03_A05
PRM-03	PRM-03_A06
PRM-04	PRM-04_A01
PRM-04	PRM-04_A02
PRM-04	PRM-04_A03
PRM-04	PRM-04_A04
PRM-04	PRM-04_A05
PRM-04	PRM-04_A06

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

PRM-04	PRM-04_A13
PRM-05	PRM-05_A01
PRM-05	PRM-05_A02
PRM-05	PRM-05_A03
PRM-06	PRM-06_A01
PRM-06	PRM-06_A02
PRM-06	PRM-06_A03
PRM-06	PRM-06_A04
PRM-06	PRM-06_A05
PRM-06	PRM-06_A06
PRM-06	PRM-06_A07
PRM-07	PRM-07_A01
PRM-07	PRM-07_A02
PRM-07	PRM-07_A03
PRM-07	PRM-07_A04
PRM-07	PRM-07_A05
PRM-07	PRM-07_A06
PRM-07	PRM-07_A07
PRM-07	PRM-07_A08
PRM-07	PRM-07_A09
PRM-07	PRM-07_A10
PRM-07	PRM-07_A11
PRM-07	PRM-07_A12
PRM-08	PRM-08_A01
PRM-08	PRM-08_A02
PRM-08	PRM-08_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

RSK-01	RSK-01_A07
RSK-01	RSK-01_A08
RSK-01	RSK-01_A09
RSK-01	RSK-01_A10
RSK-01	RSK-01_A11
RSK-01.1	RSK-01.1_A01
RSK-01.1	RSK-01.1_A02
RSK-01.1	RSK-01.1_A03
RSK-01.1	RSK-01.1_A04
RSK-01.1	RSK-01.1_A05
RSK-01.1	RSK-01.1_A06
RSK-01.1	RSK-01.1_A07
RSK-01.1	RSK-01.1_A08
RSK-01.1	RSK-01.1_A09
RSK-01.1	RSK-01.1_A10
RSK-01.1	RSK-01.1_A11
RSK-01.1	RSK-01.1_A12
RSK-01.1	RSK-01.1_A13
RSK-01.2	RSK-01.2_A01
RSK-01.2	RSK-01.2_A02
RSK-01.2	RSK-01.2_A03
RSK-01.3	RSK-01.3_A01
RSK-01.4	RSK-01.4_A01
RSK-02	RSK-02_A01
RSK-02	RSK-02_A02
RSK-02	RSK-02_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

RSK-04	RSK-04_A04
RSK-04	RSK-04_A05
RSK-04	RSK-04_A06
RSK-04	RSK-04_A07
RSK-04	RSK-04_A08
RSK-04	RSK-04_A09
RSK-04	RSK-04_A10
RSK-04	RSK-04_A11
RSK-04	RSK-04_A12
RSK-04	RSK-04_A13
RSK-04	RSK-04_A14
RSK-04	RSK-04_A15
RSK-04	RSK-04_A16
RSK-04	RSK-04_A17
RSK-04	RSK-04_A18
RSK-04.1	RSK-04.1_A01
RSK-05	RSK-05_A01
RSK-06.1	RSK-06.1_A01
RSK-06.1	RSK-06.1_A02
RSK-06.1	RSK-06.1_A03
RSK-06.1	RSK-06.1_A04
RSK-06.2	RSK-06.2_A01
RSK-07	RSK-07_A01
RSK-08	RSK-08_A01
RSK-09	RSK-09_A01
RSK-09	RSK-09_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

RSK-09	RSK-09_A09
RSK-09	RSK-09_A10
RSK-09	RSK-09_A11
RSK-09	RSK-09_A12
RSK-09	RSK-09_A13
RSK-09	RSK-09_A14
RSK-09	RSK-09_A15
RSK-09	RSK-09_A16
RSK-09	RSK-09_A17
RSK-09	RSK-09_A18
RSK-09	RSK-09_A19
RSK-09	RSK-09_A20
RSK-09	RSK-09_A21
RSK-09.1	RSK-09.1_A01
RSK-09.1	RSK-09.1_A02
RSK-09.1	RSK-09.1_A03
RSK-09.1	RSK-09.1_A04
RSK-09.1	RSK-09.1_A05
RSK-09.1	RSK-09.1_A06
RSK-09.2	RSK-09.2_A01
RSK-10	RSK-10_A01
RSK-10	RSK-10_A02
RSK-10	RSK-10_A03
RSK-11	RSK-11_A01
RSK-11	RSK-11_A02
RSK-11	RSK-11_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

SEA-01	SEA-01_A04
SEA-01	SEA-01_A05
SEA-01	SEA-01_A06
SEA-01	SEA-01_A07
SEA-01	SEA-01_A08
SEA-01	SEA-01_A09
SEA-01	SEA-01_A10
SEA-01	SEA-01_A11
SEA-01	SEA-01_A12
SEA-01	SEA-01_A13
SEA-01	SEA-01_A14
SEA-01	SEA-01_A15
SEA-01	SEA-01_A16
SEA-01	SEA-01_A17
SEA-01	SEA-01_A18
SEA-01	SEA-01_A19
SEA-01.1	SEA-01.1_A01
SEA-01.1	SEA-01.1_A02
SEA-02	SEA-02_A01
SEA-02	SEA-02_A02
SEA-02	SEA-02_A03
SEA-02	SEA-02_A04
SEA-02	SEA-02_A05
SEA-02	SEA-02_A06
SEA-02	SEA-02_A07
SEA-02	SEA-02_A08

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

SEA-02	SEA-02_A15
SEA-02	SEA-02_A16
SEA-02	SEA-02_A17
SEA-02	SEA-02_A18
SEA-02	SEA-02_A19
SEA-02	SEA-02_A20
SEA-02.1	SEA-02.1_A01
SEA-02.2	SEA-02.2
SEA-02.2	SEA-02.2_A02
SEA-02.3	SEA-02.3_A01
SEA-02.3	SEA-02.3_A02
SEA-03	SEA-03_A01
SEA-03	SEA-03_A02
SEA-03	SEA-03_A03
SEA-03	SEA-03_A04
SEA-03	SEA-03_A05
SEA-03	SEA-03_A06
SEA-03	SEA-03_A07
SEA-03.1	SEA-03.1_A01
SEA-03.1	SEA-03.1_A02
SEA-03.1	SEA-03.1_A03
SEA-03.2	SEA-03.2_A01
SEA-03.2	SEA-03.2_A02
SEA-03.2	SEA-03.2_A03
SEA-03.2	SEA-03.2_A04
SEA-03.2	SEA-03.2_A05

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

SEA-05	SEA-05_A02
SEA-06	SEA-06_A01
SEA-06	SEA-06_A02
SEA-07	SEA-07_A01
SEA-07	SEA-07_A02
SEA-07	SEA-07_A03
SEA-07	SEA-07_A04
SEA-07.1	SEA-07.1_A01
SEA-07.1	SEA-07.1_A02
SEA-07.1	SEA-07.1_A03
SEA-07.2	SEA-07.2_A01
SEA-07.2	SEA-07.2_A02
SEA-07.2	SEA-07.2_A03
SEA-07.2	SEA-07.2_A04
SEA-07.2	SEA-07.2_A05
SEA-07.2	SEA-07.2_A06
SEA-07.2	SEA-07.2_A07
SEA-07.2	SEA-07.2_A08
SEA-07.2	SEA-07.2_A09
SEA-07.2	SEA-07.2_A10
SEA-07.2	SEA-07.2_A11
SEA-07.3	SEA-07.3_A01
SEA-07.3	SEA-07.3_A02
SEA-07.3	SEA-07.3_A03
SEA-08	SEA-08_A01
SEA-08	SEA-08_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

SEA-08.1	SEA-08.1_A05
SEA-08.1	SEA-08.1_A06
SEA-08.1	SEA-08.1_A07
SEA-08.1	SEA-08.1_A08
SEA-08.1	SEA-08.1_A09
SEA-08.1	SEA-08.1_A10
SEA-08.1	SEA-08.1_A11
SEA-08.1	SEA-08.1_A12
SEA-09	SEA-09_A01
SEA-09	SEA-09_A02
SEA-09.1	SEA-09.1_A01
SEA-10	SEA-10_A01
SEA-10	SEA-10_A02
SEA-11	SEA-11_A01
SEA-11	SEA-11_A02
SEA-11	SEA-11_A03
SEA-11	SEA-11_A04
SEA-11	SEA-11_A05
SEA-11	SEA-11_A06
SEA-11	SEA-11_A07
SEA-12	SEA-12_A01
SEA-12	SEA-12_A02
SEA-12	SEA-12_A03
SEA-13	SEA-13_A01
SEA-13	SEA-13_A02
SEA-13	SEA-13_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

SEA-14.1	SEA-14.1_A01
SEA-14.1	SEA-14.1_A02
SEA-14.1	SEA-14.1_A03
SEA-14.1	SEA-14.1_A04
SEA-14.1	SEA-14.1_A05
SEA-14.1	SEA-14.1_A06
SEA-14.2	SEA-14.2_A01
SEA-14.2	SEA-14.2_A02
SEA-14.2	SEA-14.2_A03
SEA-15	SEA-15_A01
SEA-15	SEA-15_A02
SEA-15	SEA-15_A03
SEA-15	SEA-15_A04
SEA-15	SEA-15_A05
SEA-15	SEA-15_A06
SEA-15	SEA-15_A07
SEA-15	SEA-15_A08
SEA-15	SEA-15_A09
SEA-16	SEA-16_A01
SEA-16	SEA-16_A02
SEA-16	SEA-16_A03
SEA-16	SEA-16_A04
SEA-17	SEA-17_A01
SEA-18	SEA-18_A01
SEA-18	SEA-18_A02
SEA-18	SEA-18_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

SEA-18	SEA-18_A10
SEA-18	SEA-18_A11
SEA-18.1	SEA-18.1_A01
SEA-18.2	SEA-18.2_A01
SEA-19	SEA-19_A01
SEA-20	SEA-20_A01
SEA-20	SEA-20_A02
OPS-01	OPS-01_A01
OPS-01	OPS-01_A02
OPS-01.1	OPS-01.1_A01
OPS-01.1	OPS-01.1_A02
OPS-01.1	OPS-01.1_A03
OPS-01.1	OPS-01.1_A04
OPS-01.1	OPS-01.1_A05
OPS-01.1	OPS-01.1_A06
OPS-01.1	OPS-01.1_A07
OPS-01.1	OPS-01.1_A08
OPS-01.1	OPS-01.1_A09
OPS-02	OPS-02_A01
OPS-02	OPS-02_A02
OPS-02	OPS-02_A03
OPS-03	OPS-03_A01
OPS-03	OPS-03_A02
OPS-04	OPS-04_A01
OPS-04	OPS-04_A02
OPS-04	OPS-04_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

SAT-02	SAT-02_A02
SAT-02	SAT-02_A03
SAT-02	SAT-02_A04
SAT-02	SAT-02_A05
SAT-02	SAT-02_A06
SAT-02	SAT-02_A07
SAT-02	SAT-02_A08
SAT-02	SAT-02_A09
SAT-02	SAT-02_A10
SAT-02	SAT-02_A11
SAT-02	SAT-02_A12
SAT-02	SAT-02_A13
SAT-02	SAT-02_A14
SAT-02	SAT-02_A15
SAT-02	SAT-02_A16
SAT-02	SAT-02_A17
SAT-02	SAT-02_A18
SAT-02	SAT-02_A19
SAT-02	SAT-02_A20
SAT-02	SAT-02_A21
SAT-02	SAT-02_A22
SAT-02.1	SAT-02.1_A01
SAT-02.1	SAT-02.1_A02
SAT-02.1	SAT-02.1_A03
SAT-02.1	SAT-02.1_A04
SAT-02.1	SAT-02.1_A05

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

SAT-02.2	SAT-02.2_A04
SAT-02.2	SAT-02.2_A05
SAT-02.2	SAT-02.2_A06
SAT-02.2	SAT-02.2_A07
SAT-03	SAT-03_A01
SAT-03	SAT-03_A02
SAT-03	SAT-03_A03
SAT-03	SAT-03_A04
SAT-03	SAT-03_A05
SAT-03	SAT-03_A06
SAT-03	SAT-03_A07
SAT-03	SAT-03_A08
SAT-03	SAT-03_A09
SAT-03	SAT-03_A10
SAT-03	SAT-03_A11
SAT-03	SAT-03_A12
SAT-03	SAT-03_A13
SAT-03	SAT-03_A14
SAT-03.1	SAT-03.1_A01
SAT-03.1	SAT-03.1_A02
SAT-03.2	SAT-03.2_A01
SAT-03.2	SAT-03.2_A02
SAT-03.2	SAT-03.2_A03
SAT-03.3	SAT-03.3_A01
SAT-03.3	SAT-03.3_A02
SAT-03.3	SAT-03.3_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

SAT-03.7	SAT-03.7_A01
SAT-03.8	SAT-03.8_A01
SAT-04	SAT-04_A01
SAT-04	SAT-04_A02
SAT-04	SAT-04_A03
SAT-04	SAT-04_A04
TDA-01	TDA-01_A01
TDA-01	TDA-01_A02
TDA-01	TDA-01_A03
TDA-01	TDA-01_A04
TDA-01	TDA-01_A05
TDA-01	TDA-01_A06
TDA-01	TDA-01_A07
TDA-01	TDA-01_A08
TDA-01	TDA-01_A09
TDA-01	TDA-01_A10
TDA-01	TDA-01_A11
TDA-01	TDA-01_A12
TDA-01	TDA-01_A13
TDA-01	TDA-01_A14
TDA-01	TDA-01_A15
TDA-01	TDA-01_A16
TDA-01	TDA-01_A17
TDA-01	TDA-01_A18
TDA-01	TDA-01_A19
TDA-01	TDA-01_A20

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TDA-01	TDA-01_A27
TDA-01.1	TDA-01.1_A01
TDA-01.1	TDA-01.1_A02
TDA-01.2	TDA-01.2_A01
TDA-01.3	TDA-01.3_A01
TDA-02	TDA-02_A01
TDA-02	TDA-02_A02
TDA-02	TDA-02_A03
TDA-02	TDA-02_A04
TDA-02	TDA-02_A05
TDA-02	TDA-02_A06
TDA-02	TDA-02_A07
TDA-02	TDA-02_A08
TDA-02	TDA-02_A09
TDA-02	TDA-02_A10
TDA-02	TDA-02_A11
TDA-02	TDA-02_A12
TDA-02	TDA-02_A13
TDA-02	TDA-02_A14
TDA-02	TDA-02_A15
TDA-02	TDA-02_A16
TDA-02.1	TDA-02.1_A01
TDA-02.1	TDA-02.1_A02
TDA-02.1	TDA-02.1_A03
TDA-02.1	TDA-02.1_A04
TDA-02.2	TDA-02.2_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TDA-02.3	TDA-02.3_A07
TDA-02.4	TDA-02.4_A01
TDA-02.4	TDA-02.4_A02
TDA-02.4	TDA-02.4_A03
TDA-02.5	TDA-02.5_A01
TDA-02.5	TDA-02.5_A02
TDA-02.6	TDA-02.6_A01
TDA-02.7	TDA-02.7_A01
TDA-02.7	TDA-02.7_A02
TDA-02.7	TDA-02.7_A03
TDA-02.7	TDA-02.7_A04
TDA-02.7	TDA-02.7_A05
TDA-02.7	TDA-02.7_A06
TDA-03	TDA-03_A01
TDA-03	TDA-03_A02
TDA-03	TDA-03_A03
TDA-03.1	TDA-03.1_A01
TDA-03.1	TDA-03.1_A02
TDA-03.1	TDA-03.1_A03
TDA-03.1	TDA-03.1_A04
TDA-03.1	TDA-03.1_A05
TDA-03.1	TDA-03.1_A06
TDA-03.1	TDA-03.1_A07
TDA-04	TDA-04_A01
TDA-04	TDA-04_A02
TDA-04	TDA-04_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TDA-04	TDA-04_A10
TDA-04	TDA-04_A11
TDA-04	TDA-04_A12
TDA-04	TDA-04_A13
TDA-04	TDA-04_A14
TDA-04	TDA-04_A15
TDA-04	TDA-04_A16
TDA-04	TDA-04_A17
TDA-04	TDA-04_A18
TDA-04	TDA-04_A19
TDA-04	TDA-04_A20
TDA-04	TDA-04_A21
TDA-04	TDA-04_A22
TDA-04.1	TDA-04.1_A01
TDA-04.1	TDA-04.1_A02
TDA-04.1	TDA-04.1_A03
TDA-04.1	TDA-04.1_A04
TDA-04.1	TDA-04.1_A05
TDA-04.2	TDA-04.2_A01
TDA-05	TDA-05_A01
TDA-05	TDA-05_A02
TDA-05	TDA-05_A03
TDA-05	TDA-05_A04
TDA-05	TDA-05_A05
TDA-05	TDA-05_A06
TDA-05.1	TDA-05.1_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TDA-06	TDA-06_A06
TDA-06	TDA-06_A07
TDA-06	TDA-06_A08
TDA-06	TDA-06_A09
TDA-06	TDA-06_A10
TDA-06	TDA-06_A11
TDA-06	TDA-06_A12
TDA-06	TDA-06_A13
TDA-06	TDA-06_A14
TDA-06	TDA-06_A15
TDA-06	TDA-06_A16
TDA-06	TDA-06_A17
TDA-06	TDA-06_A18
TDA-06.1	TDA-06.1_A01
TDA-06.1	TDA-06.1_A02
TDA-06.1	TDA-06.1_A03
TDA-06.1	TDA-06.1_A04
TDA-06.1	TDA-06.1_A05
TDA-06.1	TDA-06.1_A06
TDA-06.1	TDA-06.1_A07
TDA-06.1	TDA-06.1_A08
TDA-06.1	TDA-06.1_A09
TDA-06.2	TDA-06.2_A01
TDA-06.3	TDA-06.3_A01
TDA-06.4	TDA-06.4_A01
TDA-06.5	TDA-06.5_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TDA-08	TDA-08_A06
TDA-08	TDA-08_A07
TDA-08	TDA-08_A08
TDA-08	TDA-08_A09
TDA-08.1	TDA-08.1_A01
TDA-09	TDA-09_A01
TDA-09	TDA-09_A02
TDA-09	TDA-09_A03
TDA-09	TDA-09_A04
TDA-09	TDA-09_A05
TDA-09	TDA-09_A06
TDA-09	TDA-09_A07
TDA-09	TDA-09_A08
TDA-09	TDA-09_A09
TDA-09	TDA-09_A10
TDA-09	TDA-09_A11
TDA-09	TDA-09_A12
TDA-09	TDA-09_A13
TDA-09	TDA-09_A14
TDA-09	TDA-09_A15
TDA-09	TDA-09_A16
TDA-09.1	TDA-09.1_A01
TDA-09.2	TDA-09.2_A01
TDA-09.2	TDA-09.2_A02
TDA-09.3	TDA-09.3_A01
TDA-09.3	TDA-09.3_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TDA-09.5	TDA-09.5_A03
TDA-09.5	TDA-09.5_A04
TDA-09.6	TDA-09.6_A01
TDA-09.7	TDA-09.7_A01
TDA-09.7	TDA-09.7_A02
TDA-09.7	TDA-09.7_A03
TDA-10	TDA-10_A01
TDA-10	TDA-10_A02
TDA-10	TDA-10_A03
TDA-10	TDA-10_A04
TDA-10.1	TDA-10.1_A01
TDA-11	TDA-11_A01
TDA-11	TDA-11_A02
TDA-11	TDA-11_A03
TDA-11	TDA-11_A04
TDA-11	TDA-11_A05
TDA-11	TDA-11_A06
TDA-11	TDA-11_A07
TDA-11	TDA-11_A08
TDA-11	TDA-11_A09
TDA-11	TDA-11_A10
TDA-11	TDA-11_A11
TDA-11	TDA-11_A12
TDA-11	TDA-11_A13
TDA-11	TDA-11_A14
TDA-11	TDA-11_A15

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TDA-11.1	TDA-11.1_A02
TDA-12	TDA-12_A01
TDA-12	TDA-12_A02
TDA-12	TDA-12_A03
TDA-12	TDA-12_A04
TDA-12	TDA-12_A05
TDA-12	TDA-12_A06
TDA-12	TDA-12_A07
TDA-13	TDA-13_A01
TDA-13	TDA-13_A02
TDA-13	TDA-13_A03
TDA-14	TDA-14_A01
TDA-14	TDA-14_A02
TDA-14	TDA-14_A03
TDA-14	TDA-14_A04
TDA-14	TDA-14_A05
TDA-14	TDA-14_A06
TDA-14	TDA-14_A07
TDA-14	TDA-14_A08
TDA-14	TDA-14_A09
TDA-14	TDA-14_A10
TDA-14	TDA-14_A11
TDA-14	TDA-14_A12
TDA-14	TDA-14_A13
TDA-14	TDA-14_A14
TDA-14	TDA-14_A15

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TDA-14	TDA-14_A22
TDA-14	TDA-14_A23
TDA-14	TDA-14_A24
TDA-14.1	TDA-14.1_A01
TDA-14.2	TDA-14.2_A01
TDA-14.2	TDA-14.2_A02
TDA-14.2	TDA-14.2_A03
TDA-14.2	TDA-14.2_A04
TDA-15	TDA-15_A01
TDA-15	TDA-15_A02
TDA-15	TDA-15_A03
TDA-15	TDA-15_A04
TDA-15	TDA-15_A05
TDA-15	TDA-15_A06
TDA-15	TDA-15_A07
TDA-15	TDA-15_A08
TDA-15	TDA-15_A09
TDA-15	TDA-15_A10
TDA-15	TDA-15_A11
TDA-15	TDA-15_A12
TDA-15	TDA-15_A13
TDA-15	TDA-15_A14
TDA-15	TDA-15_A15
TDA-15	TDA-15_A16
TDA-15	TDA-15_A17
TDA-15	TDA-15_A18

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TDA-17.1	TDA-17.1_A01
TDA-18	TDA-18_A01
TDA-18	TDA-18_A02
TDA-18	TDA-18_A03
TDA-19	TDA-19_A01
TDA-19	TDA-19_A02
TDA-19	TDA-19_A03
TDA-20	TDA-20_A01
TDA-20	TDA-20_A04
TDA-20.1	TDA-20.1_A01
TDA-20.2	TDA-20.2_A01
TDA-20.3	TDA-20.3_A01
TPM-01	TPM-01_A01
TPM-01	TPM-01_A02
TPM-01	TPM-01_A03
TPM-01	TPM-01_A04
TPM-01	TPM-01_A05
TPM-01	TPM-01_A06
TPM-01	TPM-01_A07
TPM-01	TPM-01_A08
TPM-01	TPM-01_A09
TPM-01	TPM-01_A10
TPM-01	TPM-01_A11
TPM-01	TPM-01_A12
TPM-01	TPM-01_A13
TPM-01	TPM-01_A14

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TPM-02	TPM-02_A03
TPM-02	TPM-02_A04
TPM-02	TPM-02_A05
TPM-02	TPM-02_A06
TPM-03	TPM-03_A01
TPM-03	TPM-03_A02
TPM-03	TPM-03_A03
TPM-03	TPM-03_A04
TPM-03	TPM-03_A05
TPM-03	TPM-03_A06
TPM-03	TPM-03_A07
TPM-03	TPM-03_A08
TPM-03	TPM-03_A09
TPM-03	TPM-03_A10
TPM-03	TPM-03_A11
TPM-03	TPM-03_A12
TPM-03	TPM-03_A13
TPM-03	TPM-03_A14
TPM-03	TPM-03_A15
TPM-03	TPM-03_A16
TPM-03	TPM-03_A17
TPM-03.1	TPM-03.1_A01
TPM-03.1	TPM-03.1_A02
TPM-03.1	TPM-03.1_A03
TPM-03.1	TPM-03.1_A04
TPM-03.2	TPM-03.2_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TPM-03.3	TPM-03.3_A06
TPM-03.3	TPM-03.3_A07
TPM-03.3	TPM-03.3_A08
TPM-04	TPM-04_A01
TPM-04	TPM-04_A02
TPM-04	TPM-04_A03
TPM-04	TPM-04_A04
TPM-04	TPM-04_A05
TPM-04	TPM-04_A06
TPM-04	TPM-04_A07
TPM-04	TPM-04_A08
TPM-04.1	TPM-04.1_A01
TPM-04.1	TPM-04.1_A02
TPM-04.1	TPM-04.1_A03
TPM-04.2	TPM-04.2_A01
TPM-04.2	TPM-04.2_A02
TPM-04.3	TPM-04.3_A01
TPM-04.3	TPM-04.3_A02
TPM-04.3	TPM-04.3_A03
TPM-04.4	TPM-04.4_A01
TPM-04.4	TPM-04.4_A02
TPM-04.4	TPM-04.4_A03
TPM-04.4	TPM-04.4_A04
TPM-04.4	TPM-04.4_A05
TPM-05	TPM-05_A01
TPM-05	TPM-05_A02

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

TPM-05.6	TPM-05.4_A03
TPM-05.7	TPM-05.7_A01
TPM-06	TPM-06_A01
TPM-07	TPM-07_A01
TPM-07	TPM-07_A02
TPM-08	TPM-08_A01
TPM-08	TPM-08_A02
TPM-08	TPM-08_A03
TPM-08	TPM-08_A04
TPM-09	TPM-09_A01
TPM-10	TPM-10_A01
TPM-10	TPM-10_A02
TPM-10	TPM-10_A03
TPM-10	TPM-10_A04
TPM-11	TPM-11_A01
THR-01	THR-01_A01
THR-01	THR-01_A02
THR-01	THR-01_A03
THR-01	THR-01_A04
THR-01	THR-01_A05
THR-01	THR-01_A06
THR-01	THR-01_A07
THR-01	THR-01_A08
THR-01	THR-01_A09
THR-01	THR-01_A10
THR-01	THR-01_A11

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

THR-03	THR-03_A06
THR-03	THR-03_A07
THR-03	THR-03_A08
THR-03	THR-03_A09
THR-03	THR-03_A10
THR-03	THR-03_A11
THR-03	THR-03_A12
THR-03	THR-03_A13
THR-03	THR-03_A14
THR-03	THR-03_A15
THR-03	THR-03_A16
THR-04	THR-04_A01
THR-04	THR-04_A02
THR-05	THR-05_A01
THR-05	THR-05_A02
THR-05	THR-05_A03
THR-05	THR-05_A04
THR-06	THR-06_A01
THR-07	THR-07_A01
THR-07	THR-07_A02
THR-07	THR-07_A03
THR-07	THR-07_A04
THR-07	THR-07_A05
THR-07	THR-07_A06
THR-07	THR-07_A07
THR-07	THR-07_A08

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

VPM-01	VPM-01_A02
VPM-01	VPM-01_A03
VPM-01	VPM-01_A04
VPM-01	VPM-01_A05
VPM-01	VPM-01_A06
VPM-01	VPM-01_A07
VPM-01	VPM-01_A08
VPM-01	VPM-01_A09
VPM-01	VPM-01_A10
VPM-01	VPM-01_A11
VPM-01	VPM-01_A12
VPM-01	VPM-01_A13
VPM-01	VPM-01_A14
VPM-01.1	VPM-01.1_A01
VPM-01.1	VPM-01.1_A02
VPM-01.1	VPM-01.1_A03
VPM-01.1	VPM-01.1_A04
VPM-01.1	VPM-01.1_A05
VPM-01.1	VPM-01.1_A06
VPM-01.1	VPM-01.1_A07
VPM-02	VPM-02_A01
VPM-02	VPM-02_A02
VPM-03	VPM-03_A01
VPM-04	VPM-04_A01
VPM-04	VPM-04_A02
VPM-04	VPM-04_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

VPM-05	VPM-05_A04
VPM-05	VPM-05_A05
VPM-05	VPM-05_A06
VPM-05	VPM-05_A07
VPM-05	VPM-05_A08
VPM-05	VPM-05_A09
VPM-05	VPM-05_A10
VPM-05	VPM-05_A11
VPM-05	VPM-05_A12
VPM-05	VPM-05_A13
VPM-05.1	VPM-05.1_A01
VPM-05.1	VPM-05.1_A02
VPM-05.1	VPM-05.1_A03
VPM-05.1	VPM-05.1_A04
VPM-05.2	VPM-05.2_A01
VPM-05.2	VPM-05.2_A02
VPM-05.2	VPM-05.2_A03
VPM-05.2	VPM-05.2_A04
VPM-05.2	VPM-05.2_A05
VPM-05.3	VPM-05.3_A01
VPM-05.3	VPM-05.3_A02
VPM-05.3	VPM-05.3_A03
VPM-05.4	VPM-05.4_A01
VPM-05.4	VPM-05.4_A02
VPM-05.4	VPM-05.4_A03
VPM-05.4	VPM-05.4_A04

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

VPM-06	VPM-06_A04
VPM-06	VPM-06_A05
VPM-06	VPM-06_A06
VPM-06	VPM-06_A07
VPM-06	VPM-06_A08
VPM-06	VPM-06_A09
VPM-06	VPM-06_A10
VPM-06	VPM-06_A11
VPM-06	VPM-06_A12
VPM-06	VPM-06_A13
VPM-06	VPM-06_A14
VPM-06	VPM-06_A15
VPM-06	VPM-06_A16
VPM-06	VPM-06_A17
VPM-06	VPM-06_A18
VPM-06.1	VPM-06.1_A01
VPM-06.1	VPM-06.1_A03
VPM-06.2	VPM-06.2_A01
VPM-06.3	VPM-06.3_A01
VPM-06.3	VPM-06.3_A02
VPM-06.3	VPM-06.3_A03
VPM-06.4	VPM-06.4_A01
VPM-06.4	VPM-06.4_A02
VPM-06.5	VPM-06.5_A01
VPM-06.5	VPM-06.5_A02
VPM-06.5	VPM-06.5_A03

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

VPM-07	VPM-07_A01
VPM-07	VPM-07_A02
VPM-07	VPM-07_A03
VPM-07	VPM-07_A04
VPM-07	VPM-07_A05
VPM-07	VPM-07_A06
VPM-07	VPM-07_A07
VPM-07	VPM-07_A08
VPM-07.1	VPM-07.1_A01
VPM-08	VPM-08_A01
VPM-08	VPM-08_A02
VPM-08	VPM-08_A03
VPM-08	VPM-08_A04
VPM-09	VPM-09_A01
VPM-09	VPM-09_A02
VPM-10	VPM-10_A01
VPM-10	VPM-10_A02
WEB-01	WEB-01_A01
WEB-01.1	WEB-01.1_A01
WEB-02	WEB-02_A01
WEB-03	WEB-03_A01
WEB-04	WEB-04_A01
WEB-05	WEB-05_A01
WEB-06	WEB-06_A01
WEB-07	WEB-07_A01
WEB-08	WEB-08_A01

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

the cybersecurity & privacy governance program provides a description of the security program management controls in place or planned for meeting those requirements.
the cybersecurity & privacy governance program provides a description of the common controls in place or planned for meeting those requirements.
the cybersecurity & privacy governance program includes the identification and assignment of roles.
the cybersecurity & privacy governance program includes the identification and assignment of responsibilities.
the cybersecurity & privacy governance program addresses management commitment.
the cybersecurity & privacy governance program addresses coordination among organizational entities.
the cybersecurity & privacy governance program addresses statutory, regulatory and/or contractual compliance obligations.
the cybersecurity & privacy governance program reflects the coordination among the organizational entities responsible for cybersecurity & privacy.
the cybersecurity & privacy governance program is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations.
the frequency at which to review and update the organization-wide cybersecurity & privacy governance program is defined.
events that trigger the review and update of the organization-wide cybersecurity & privacy governance program are defined.
the cybersecurity & privacy governance program is reviewed and updated frequently.
the cybersecurity & privacy governance program is reviewed and updated following events.
an executive steering committee, or advisory board, is formed and is comprised of key cybersecurity, technology, risk, privacy and business executives.
the executive steering committee, or advisory board, coordinates cybersecurity, technology, risk, privacy and business alignment through recurring, formal meetings.
the executive steering committee, or advisory board, makes executive decisions about matters considered material to the organization's cybersecurity and privacy program.
an official to manage the governance of cybersecurity & privacy policies and procedures is defined.
security and privacy policies are developed and documented.
the cybersecurity & privacy policies addresses purpose.
the cybersecurity & privacy policies addresses scope.
the cybersecurity & privacy policies addresses roles.
the cybersecurity & privacy policies address responsibilities.
the cybersecurity & privacy policies address management commitment.
the cybersecurity & privacy policies address coordination among organizational entities.
the cybersecurity & privacy policies address compliance.
the cybersecurity & privacy policies are consistent with applicable laws, regulations and contractual obligations.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

the cybersecurity & privacy policies are reviewed and updated following events.
a senior organizational cybersecurity position is appointed.
the senior organizational cybersecurity position is provided with the mission and resources to coordinate an organization-wide cybersecurity program.
the senior organizational cybersecurity position is provided with the mission and resources to develop an organization-wide cybersecurity program.
the senior organizational cybersecurity position is provided with the mission and resources to implement an organization-wide cybersecurity program.
the senior organizational cybersecurity position is provided with the mission and resources to maintain an organization-wide cybersecurity program.
the cybersecurity & privacy governance program includes the identification and assignment of roles.
the cybersecurity & privacy governance program includes the identification and assignment of responsibilities.
a formal organization structure is published.
an individual's chain of command is clearly delineated.
cybersecurity measures of performance are developed.
cybersecurity measures of performance are monitored.
the results of cybersecurity measures of performance are reported.
privacy measures of performance are developed.
privacy measures of performance are monitored.
the results of privacy measures of performance are reported.
Key Performance Indicators (KPIs) are developed to assist organizational management in performance monitoring and trend analysis of specific aspects of the organization's cybersecurity & privacy program.
Key Risk Indicators (KRIs) are developed to assist senior management in performance monitoring and trend analysis of specific aspects of the organization's cybersecurity & privacy program.
relevant law enforcement and/or regulatory bodies are identified that necessitate communications.
contacts with relevant law enforcement and/or regulatory bodies are established and documented.
contact is established and institutionalized with selected groups and associations within the cybersecurity & privacy community to facilitate ongoing security education and training for organizational personnel.
contact is established and institutionalized with selected groups and associations within the cybersecurity & privacy community to maintain currency with recommended security practices, techniques and technologies.
contact is established and institutionalized with selected groups and associations within the cybersecurity & privacy community to share current security information, including threats, vulnerabilities and incidents.
the organization's mission is clearly defined and documented.
the organization's executive leadership defines and documents a formal business strategy that is used to provide operational guidance to key business leaders across the organization.
security and privacy-related control objectives are established as the basis for the selection, implementation and management of the organization’s internal control system.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

systems or system components supporting mission-essential services or functions are defined.
systems or system components supporting mission-essential services or functions are analyzed to ensure that the information resources are being used in a manner that is consistent with their intended purpose.
an executive steering committee, or advisory board, evaluates business practices for possible forced exfiltration of sensitive / regulated information (e.g., Intellectual Property (IP)) to a host government for purposes of market access or market management practices.
measures exist for the executive steering committee, or advisory board, to proactively identify and evaluate host nation business practices to identify potential instances that exist for forced exfiltration of sensitive / regulated information (e.g., Intellectual Property (IP)) to the host government for purposes of market access or market management practices.
actions are taken to prevent and/or block potential instances that enable the forced exfiltration of sensitive / regulated information (e.g., Intellectual Property (IP)) to the host government for purposes of market access or market management practices.
an executive steering committee, or advisory board, evaluates business practices for possible instances where host nation business practices could leverage the organization's technology assets for economic or political espionage and/or cyberwarfare activities.
measures exist for the executive steering committee, or advisory board, to proactively identify and evaluate host nation business practices to leverage the organization's technology assets for economic or political espionage and/or cyberwarfare activities.
actions are taken to prevent and/or block potential instances where host nation business practices could leverage the organization's technology assets for economic or political espionage and/or cyberwarfare activities.
the executive steering committee, or advisory board, directs organization leadership to incorporate cybersecurity and privacy principles into Business As Usual (BAU) practices.
cybersecurity incidents are reviewed to identify incidents that occurred due to cybersecurity and/or privacy principles not being adopted as Business As Usual (BAU) practices.
identified deficiencies of cybersecurity and/or privacy principles not being adopted as Business As Usual (BAU) practices are tracked via a Plan of Action and Milestones (POA&M), or risk register, through remediation.
roles and responsibilities exist to compel data and/or process owners to operationalize cybersecurity and privacy practices for each system, application and/or service under their control.
Individual Contributor (IC) performance reviews cover how data and/or process owners operationalized cybersecurity and privacy practices for each system, application and/or service under their control.
roles and responsibilities exist to compel data and/or process owners to select required cybersecurity and privacy controls for each system, application and/or service under their control.
Individual Contributor (IC) performance reviews cover how data and/or process owners select required cybersecurity and privacy controls for each system, application and/or service under their control.
roles and responsibilities exist to compel data and/or process owners to implement required cybersecurity and privacy controls for each system, application and/or service under their control.
Individual Contributor (IC) performance reviews cover how data and/or process owners implement required cybersecurity and privacy controls for each system, application and/or service under their control.
roles and responsibilities exist to compel data and/or process owners to assess if required cybersecurity and privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.
Individual Contributor (IC) performance reviews cover how data and/or process owners assess if required cybersecurity and privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.
roles and responsibilities exist to compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.
Individual Contributor (IC) performance reviews cover how data and/or process owners obtain authorization for the production use of each system, application and/or service under their control.
roles and responsibilities exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity and privacy controls are operating as intended.
Individual Contributor (IC) performance reviews cover how data and/or process owners monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity and privacy controls are operating as intended.
Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific policies, standards and procedures are developed and documented.
Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific policies, standards and procedures are implemented effectively.
the organization analyzes its business practices to determine applicable statutory, regulatory and/or contractual obligations for Artificial Intelligence (AI) and Autonomous Technologies (AAT).

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

a compliance catalog of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific laws, regulations and contractual obligations are documented.
the organization maps its risk catalog to its compliance catalog for Artificial Intelligence (AI) and Autonomous Technologies (AAT).
roles and responsibilities exist to compel data and/or process owners to select required cybersecurity and privacy controls for Artificial Intelligence (AI) and Autonomous Technologies (AAT) under their control.
Individual Contributor (IC) performance reviews cover how data and/or process owners operationalized cybersecurity and privacy practices for Artificial Intelligence (AI) and Autonomous Technologies (AAT) under their control.
the context for the intended purpose(s) for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.
the context for the potentially beneficial use(s) for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.
the context for the legal and regulatory compliance for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.
the context for the norms and expectations for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.
the context for the proposed deployment setting(s) for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.
the mission for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.
the relevant goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is clearly documented.
capabilities for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is benchmarked.
targeted usage for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is benchmarked.
goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is benchmarked.
expected benefits for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is benchmarked.
expected costs for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is benchmarked.
documented methods exist to viably assess the potential benefits of Artificial Intelligence (AI) and Autonomous Technologies (AAT).
documented methods exist to viably assess the potential costs, including non-monetary costs, resulting from expected or realized Artificial Intelligence (AI)-related errors or system functionality and trustworthiness.
the scope for Artificial Intelligence (AI) and Autonomous Technologies (AAT) is defined.
a risk catalog of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific risks is documented.
a compliance catalog of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific laws, regulations and contractual obligations are documented.
a Third-Party Service Provider (TSP) catalog that includes Software as a Service (SaaS) is documented.
the organization maps its risk catalog across its compliance and Third-Party Service Provider (TSP) catalog for Artificial Intelligence (AI) and Autonomous Technologies (AAT) to determine the scope and potential impact of AAT-related risks.
roles and responsibilities for role-based cybersecurity & privacy training are defined for Artificial Intelligence (AI) and Autonomous Technologies (AAT) internal and external stakeholders.
the frequency at which to provide role-based cybersecurity & privacy training to Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders after initial training is defined.
events that require role-based training content for Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be updated are defined.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

the organization leverages decision makers from a diversity of expertise for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks leverage personnel
the organization leverages decision makers from a diversity of backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks leverage personnel
the organization characterizes the impacts of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals.
the organization characterizes the impact of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on groups.
the organization characterizes the impact of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on communities
the organization characterizes the impact of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on organizations.
the organization characterizes the impact of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on society.
the potential likelihood is documented for each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.
the potential impact is documented for each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.
a documented strategy exists to implement continuously monitoring of Artificial Intelligence (AI) and Autonomous Technologies (AAT) that maximize benefits, while minimizing negative impacts.
cybersecurity & privacy roles and responsibilities are incorporated into organizational position descriptions.
users are formally made aware of their roles and responsibilities to maintain a safe and secure working environment.
acknowledgement of user awareness is maintained by the organization.
the frequency at which to review and update position risk designations is defined.
a risk designation is assigned to all organizational positions.
a risk catalog of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific risks is documented.
the organization maps its risk catalog, including potential impacts, to instances where Artificial Intelligence (AI) and Autonomous Technologies (AAT) is designed, developed, deployed, evaluated and used.
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability is organization-wide.
a process is implemented for ensuring that organizational plans for conducting security and/or privacy testing, training and monitoring activities associated with organizational systems are developed.
a process is implemented for ensuring that organizational plans for conducting security and/or privacy testing, training and monitoring activities associated with organizational systems are maintained.
a process is implemented for ensuring that organizational plans for conducting security and/or privacy testing, training and monitoring activities associated with organizational systems continue to be executed.
the authorization processes are integrated into an organization-wide risk management program.
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability evaluates Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy characteristics.
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability documents test sets used during AI TEVV.
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability documents metrics used during AI TEVV.
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability documents details about the tools used during AI TEVV.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability is integrated into an organization-wide risk management program.
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability examines risks associated with transparency and accountability of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability includes a Data Protection Impact Assessment (DPIA) to identify and remediate reasonably-expected risks to Personal Data (PD).
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability includes examining fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability includes validating the engineering model used in the design of the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability includes a determination on the viability of the proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).
After Action Reviews (AARs), or similar lessons learned exercises, are conducted after each Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) cycle to evaluate the effectiveness of the AI TEVV processes.
results from Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) findings are evaluated against Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related performance demonstrated for conditions similar to deployment settings.
results from Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) findings are evaluated against Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related assurance criteria demonstrated for conditions similar to deployment settings.
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability includes proactive and continuous monitoring of deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).
the organization's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability integrates continual improvements for deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).
roles and responsibilities exist to compel data and/or process owners to compel robust, ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.
Individual Contributor (IC) performance reviews cover how data and/or process owners conducted engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.
roles and responsibilities exist to compel data and/or process owners to regularly collect, consider, prioritize and integrate risk-related feedback from those external to the team that developed or deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).
Individual Contributor (IC) performance reviews cover how data and/or process owners regularly collected, considered, prioritized and integrated risk-related feedback on Artificial Intelligence (AI) and Autonomous Technologies (AAT).
independent assessors and/or internal stakeholders, who did not serve as front-line developers, are utilized for regular assessments and updates of deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).
the organization collects feedback from end users and impacted communities into Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related system evaluation metrics.
evaluation metrics from end users and impacted communities are integrated into Artificial Intelligence (AI) and Autonomous Technologies (AAT) developments.
pertinent information from Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related incidents and/or errors are communicated to relevant stakeholders, including affected communities.
an executive steering committee, or advisory board, evaluates business practices that want to or currently use Artificial Intelligence (AI) and Autonomous Technologies (AAT).
measures exist for the executive steering committee, or advisory board, to proactively identify and evaluate third-party Intellectual Property (IP) infringement risks from Artificial Intelligence (AI) and Autonomous Technologies (AAT) usage.
actions are taken to prevent and/or block Artificial Intelligence (AI) and Autonomous Technologies (AAT) capabilities that infringe upon another party's Intellectual Property (IP).
stakeholder competencies, skills and capacities incorporate demographic diversity.
stakeholder competencies, skills and capacities incorporate broad domain expertise.
stakeholder competencies, skills and capacities incorporate broad user experience expertise.
roles and responsibilities exist to compel data and/or process owners to be proficient in Artificial Intelligence (AI) and Autonomous Technologies (AAT).

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

an executive steering committee, or advisory board, defines criteria as to whether Artificial Intelligence (AI) and Autonomous Technologies (AAT) achieved intended purposes and stated objectives.
measures exist for the executive steering committee, or advisory board, to determine whether Artificial Intelligence (AI) and Autonomous Technologies (AAT) development or deployment should proceed.
residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers and end users of Artificial Intelligence (AI) and Autonomous Technologies (AAT) are identified.
residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers and end users of Artificial Intelligence (AI) and Autonomous Technologies (AAT) documented in a Plan of Action & Milestones (POA&M), or similar risk register.
an executive steering committee, or advisory board, defines criteria for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT).
an executive steering committee, or advisory board, assigns responsibility to responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) when designated criteria is demonstrated.
responsible party(ies) monitor the functionality and behavior of deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT) for anomalous performance or outcomes inconsistent with intended use.
a risk catalog of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-specific risks is documented.
Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are identified through consultation with domain experts and other end users.
cybersecurity & privacy controls for Artificial Intelligence (AI) and Autonomous Technologies (AAT) are regularly assessed for errors and potential impacts on affected communities.
responsible party(ies) that monitor the functionality and behavior of deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT) are trained on identifying unmeasurable risks or trustworthiness characteristics.
unmeasurable risks or trustworthiness characteristics are reported in accordance with the organization's Incident Response Plan (IRP).
responsible party(ies) gather feedback about efficacy of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related measurements.
an executive steering committee, or advisory board, assesses the efficacy of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related measurements.
input from domain experts and relevant stakeholders is utilized to validate whether the Artificial Intelligence (AI) and Autonomous Technologies (AAT) perform consistently, as intended.
an executive steering committee, or advisory board, evaluates performance improvements or declines with domain experts and relevant stakeholders to define context-relevant risks and trustworthiness issues.
the organization utilizes pre-trained models for Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related monitoring and maintenance.
the organization proactively identifies unanticipated and emergent Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.
the organization tracking existing, unanticipated and emergent Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks in a Plan of Action & Milestones (POA&M), or similar risk register.
an executive steering committee, or advisory board, evaluates business practices that could pose harm to human subjects from Artificial Intelligence (AI) and Autonomous Technologies (AAT).
measures exist for the executive steering committee, or advisory board, to implement safeguards to protect human subjects from harm due to Artificial Intelligence (AI) and Autonomous Technologies (AAT).
an executive steering committee, or advisory board, evaluates the environmental impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT).
an executive steering committee, or advisory board, evaluates the sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT).
an incident response capability exists to appropriately respond to previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.
an executive steering committee, or advisory board, tracks Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.
responsible party(ies) prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

pertinent stakeholders of critical systems, applications and services are involved in supporting the ongoing secure management of those assets.
a scalable, standardized naming convention exists for systems, applications and services that avoids asset naming conflicts.
a documented, up-to-date, complete, accurate and readily available inventory of systems and system components exists.
the system inventory includes hardware, software, firmware and documentation.
the inventory is maintained (reviewed and updated) throughout the system development life cycle.
approved systems and system components are identified.
information deemed necessary to achieve effective systems and system component accountability is defined.
the frequency at which to update the inventory of systems and system components is defined.
the inventory of systems and system components is updated per an organization-defined frequency.
the inventory of systems and system components is updated as part of component installations.
the inventory of systems and system components is updated as part of component removals.
the inventory of systems and system components is updated as part of system updates.
automated mechanisms used to detect the presence of unauthorized hardware within the system are defined.
automated mechanisms used to detect the presence of unauthorized software within the system are defined.
automated mechanisms used to detect the presence of unauthorized firmware within the system are defined.
the frequency at which automated mechanisms are used to detect the presence of unauthorized hardware, software and/or firmware within the system is defined.
automated mechanisms disable network access by unauthorized components, isolate unauthorized components and/or notify organization-defined personnel or roles.
personnel or roles to be notified when unauthorized components are detected is/are defined.
organization-defined actions are taken when unauthorized hardware, software and/or firmware is/are detected.
an inventory of system components that accurately reflects the system is developed and documented.
an inventory of system components that includes all components within the system is developed and documented.
an inventory of system components that does not include duplicate accounting of components or components assigned to any other system is developed and documented.
an inventory of system components that includes information is developed and documented.
the system component inventory is reviewed and updated frequently.
assessed component configurations are included in the system component inventory.
any approved deviations to current deployed configurations are included in the system component inventory.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

DHCP server logging is utilized to detect unknown systems.
administrative practices identify software licensing restrictions to ensure compliance with End User Licensing Agreements (EULA).
software inventories are automatically or manually reviewed for software licensing compliance.
a map of system data actions is developed and documented.
a centralized repository for the system and system component inventory is provided.
automated mechanisms used to maintain the currency of the system component inventory are defined.
automated mechanisms used to maintain the completeness of the system component inventory are defined.
automated mechanisms used to maintain the accuracy of the system component inventory are defined.
automated mechanisms used to maintain the availability of the system component inventory are defined.
automated mechanisms for tracking components are defined.
organization-defined automated mechanisms are used to support the tracking of system components by geographic location.
personnel or roles from which to receive an acknowledgement is/are defined.
system components are assigned to a system.
an acknowledgement of the component assignment is received from organization-defined personnel or roles.
name, position and/or role of data ownership is documented.
individuals responsible and accountable for administering system components are identified by organization-defined criteria in the system component inventory.
systems, system components and associated data that require valid provenance are defined.
valid provenance is documented for systems, system components and associated data.
valid provenance is monitored for systems, system components and associated data.
valid provenance is maintained for systems, system components and associated data.
supply chain elements, processes and personnel associated with systems and critical system components that require unique identification are defined.
unique identification of supply chain elements, processes and personnel is established.
unique identification of supply chain elements, processes and personnel is maintained.
systems and critical system components that require unique identification for tracking through the supply chain are defined.
the unique identification of systems and critical system components is established for tracking through the supply chain.
the unique identification of systems and critical system components is maintained for tracking through the supply chain.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

a process exists to review network diagrams for accuracy.
a process exists to update network diagrams upon technologies change.
system hardware components to be marked indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component are defined.
system hardware components are marked indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.
one or more diagrams graphically depict control applicability boundaries for systems, applications, services and third parties to clarify "in-scope versus out-of-scope" determinations.
an inventory of systems, applications and services exists for each specific statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.
inventories of systems, applications and services are kept current for each specific statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.
strict control is maintained over the internal or external distribution of any kind of sensitive/regulated media.
written management approval is obtained prior to the transfer of any sensitive / regulated media outside of the organization's facilities.
enhanced protection measures for unattended systems are implemented to protect against tampering and unauthorized access.
users are educated on the need to physically secure laptops and other mobile devices out of site when traveling, preferably in the trunk of a vehicle.
devices that capture sensitive/regulated data via direct physical interaction are appropriately protected from tampering and substitution.
mobile devices are inspected for evidence of tampering upon return from geographic regions of concern or other known hostile environments that could lead to device compromise.
mobile devices that show signs of tampering are confiscated for forensic examination.
data, documentation, tools or system components to be disposed of are defined.
techniques and methods for disposing of data, documentation, tools or system components are defined.
data, documentation, tools or system components are disposed of using techniques and methods.
system media is sanitized using sanitization techniques and procedures prior to disposal.
system media is sanitized using sanitization techniques and procedures prior to release from organizational control.
system media is sanitized using sanitization techniques and procedures prior to release for reuse.
sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information are employed.
the organization governs a process to ensure that employees return all organizational assets in their possession upon termination of employment.
the organization governs a process to ensure that third-party users return all organizational assets in their possession upon termination of contract or agreement.
facility egress points are controlled by physical security measures.
prior management authorization is required for the removal of technology assets from organizational facilities.
the organization controls and tracks technology assets entering and exiting organizational facilities.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

the use of components is monitored within the system.
the use of components is controlled within the system.
the possession of unauthorized Bluetooth and wireless devices (e.g., Near Field Communications (NFC)) is prohibited in sensitive areas.
the usage of Bluetooth and wireless devices (e.g., Near Field Communications (NFC)) is prohibited in sensitive areas, unless use is in a Radio Frequency (RF)-screened building.
the possession of unauthorized Infrared (IR) communications devices is prohibited in sensitive areas.
Infrared (IR) communications are configured to prevent line of sight and reflected use in unsecured spaces.
a tamper protection program is implemented for the system, system component or system service.
anti-tamper technologies, tools and techniques are employed throughout the system development life cycle.
systems or system components that require inspection are defined.
the frequency at which to inspect systems or system components is defined.
indications of the need for an inspection of systems or system components are defined.
systems or system components are inspected to detect tampering.
a Bring Your Own Device (BYOD) program is implemented and governed to reduce risk associated with personally-owned devices in the workplace.
Supply Chain Risk Management (SCRM) practices require the removal and prohibition of certain technology services and/or equipment that are designated as supply chain threats by a statutory or regulatory body.
security-critical or essential software is defined.
root of trust mechanisms or cryptographic signatures are identified.
the integrity of security critical or essential software is verified using root of trust mechanisms or cryptographic signatures.
implementation guidance for telecommunication equipment is established to prevent damage, unauthorized modification and potential eavesdropping.
Video Teleconference (VTC) capabilities are secured in designated conference rooms to prevent potential eavesdropping.
personnel are trained to use Video Teleconference (VTC) capabilities on endpoint devices outside of conference rooms in a secure manner that prevents eavesdropping.
Internet Protocol Telephony (IPT) is securely implemented that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.
assets are configured to prohibit the use of endpoint-based microphones and/or web cameras in secure areas or where sensitive information is discussed.
Multi-Function Devices (MFD) are securely configured according to industry-recognized secure practices for the type of device.
the organization maintains a pool of temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices).
personnel travelling overseas request and are issued a temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) when travelling to authoritarian countries with a higher-than average risk for Intellectual Property (IP) theft or espionage against individuals and private companies.
upon return from travel to authoritarian counties, the issued temporary, loaner or "travel-only" end user technology (e.g., laptops and mobile devices) is wiped / re-imaged before being re-issued.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

Radio Frequency Identification (RFID) devices are secured according to defined secure baseline configurations.
secure baseline configurations exist for contactless access control systems to protect the confidentiality and integrity of data being stored, processed and/or transmitted.
contactless access control systems that are secured according to defined secure baseline configurations.
systems, applications and services are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.
the organization utilizes a defined methodology to categorize its technology assets based on data sensitivity and criticality.
the organization utilizes a defined methodology to categorize Artificial Intelligence (AI) and Autonomous Technologies (AAT) based on data sensitivity and criticality.
cybersecurity issues are addressed in the development of a critical infrastructure and key resources protection plan.
cybersecurity issues are addressed in the documentation of a critical infrastructure and key resources protection plan.
cybersecurity issues are addressed in the update of a critical infrastructure and key resources protection plan.
privacy issues are addressed in the development of a critical infrastructure and key resources protection plan.
privacy issues are addressed in the documentation of a critical infrastructure and key resources protection plan.
privacy issues are addressed in the update of a critical infrastructure and key resources protection plan.
contingency plan development is coordinated with organizational elements responsible for related plans.
the contingency plan is coordinated with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.
the transfer of organization-defined criteria mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity is planned for.
operational continuity is sustained until full system restoration at primary processing and/or storage sites.
time period consistent with recovery time and recovery point objectives for the recovery of the system is determined.
time period consistent with recovery time and recovery point objectives for the reconstitution of the system is determined.
the recovery of the system to a known state is provided within a specified time period after a disruption, compromise or failure.
a reconstitution of the system to a known state is provided within an organization-defined time period after a disruption, compromise or failure.
the alternate storage site is configured to facilitate recovery operations in accordance with recovery time objectives.
the alternate storage site is configured to facilitate recovery operations in accordance with recovery point objectives.
systems, applications and services that support essential missions and business functions are identified.
critical system assets supporting organization-defined criteria mission and business functions are identified.
the contingency plan activation time period within which to resume all mission and business functions is defined.
the resumption of all mission and business functions are planned for within an organization-defined time period of contingency plan activation.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

the time period within which to provide contingency training after assuming a contingency role or responsibility is defined.
the frequency at which to provide training to system users with a contingency role or responsibility is defined.
the frequency at which to review and update contingency training content is defined.
events necessitating review and update of contingency training are defined.
contingency training is provided to system users consistent with assigned roles and responsibilities within an organization-defined time period of assuming a contingency role or responsibility.
contingency training is provided to system users consistent with assigned roles and responsibilities when required by system changes.
contingency training is provided to system users consistent with assigned roles and responsibilities and frequency thereafter.
the contingency plan training content is reviewed and updated frequently.
the contingency plan training content is reviewed and updated following events.
simulated events are incorporated into contingency training to facilitate effective response by personnel in crisis situations.
mechanisms used in operations are employed to provide a more thorough and realistic contingency training environment.
the frequency of testing the contingency plan for the system is defined.
tests for determining the effectiveness of the contingency plan are defined.
tests for determining readiness to execute the contingency plan are defined.
the contingency plan for the system is tested frequently.
tests are used to determine the effectiveness of the plan.
tests are used to determine the readiness to execute the plan.
contingency plan testing is coordinated with organizational elements responsible for related plans.
the contingency plan is tested at the alternate processing site to familiarize contingency personnel with the facility and available resources.
the contingency plan is tested at the alternate processing site to evaluate the capabilities of the alternate processing site to support contingency operations.
the contingency plan test results are reviewed.
corrective actions to remediate contingency plan deficiencies are initiated, if needed.
personnel or roles to review a contingency plan is/are defined.
personnel or roles to approve a contingency plan is/are defined.
key contingency personnel (identified by name and/or by role) to whom copies of the contingency plan are distributed are defined.
key contingency organizational elements to which copies of the contingency plan are distributed are defined.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

a contingency plan for the system is developed that provides metrics.
a contingency plan for the system is developed that addresses contingency roles.
a contingency plan for the system is developed that addresses contingency responsibilities.
a contingency plan for the system is developed that addresses assigned individuals with contact information.
a contingency plan for the system is developed that addresses maintaining essential mission and business functions despite a system disruption, compromise or failure.
a contingency plan for the system is developed that addresses eventual, full-system restoration without deterioration of the controls originally planned and implemented.
a contingency plan for the system is developed that addresses the sharing of contingency information.
a contingency plan for the system is developed that is reviewed by personnel or roles.
a contingency plan for the system is developed that is approved by personnel or roles.
copies of the contingency plan are distributed to key contingency personnel.
copies of the contingency plan are distributed to organizational elements.
contingency planning activities are coordinated with incident handling activities.
the contingency plan for the system is reviewed frequently.
the contingency plan is updated to address changes to the organization, system or environment of operation.
the contingency plan is updated to address problems encountered during contingency plan implementation, execution or testing.
contingency plan changes are communicated to key contingency personnel.
contingency plan changes are communicated to organizational elements.
lessons learned from contingency plan testing or actual contingency activities are incorporated into contingency testing.
lessons learned from contingency plan training or actual contingency activities are incorporated into contingency testing and training.
the contingency plan is protected from unauthorized disclosure.
the contingency plan is protected from unauthorized modification.
alternative or supplemental security mechanisms are defined.
security functions are defined.
alternative or supplemental security mechanisms are employed for satisfying security functions when the primary means of implementing the security function is unavailable or compromised.
an alternate storage site is established.
establishment of the alternate storage site includes necessary agreements to permit the storage and retrieval of system backup information.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

time period consistent with recovery time and recovery point objectives is defined.
an alternate processing site, including necessary agreements to permit the transfer and resumption of system operations for essential mission and business functions, is established within an organization-defined time period when the primary processing capabilities are unavailable.
the equipment and supplies required to transfer operations are made available at the alternate processing site or if contracts are in place to support delivery to the site within an organization-specified time period for transfer.
the equipment and supplies required to resume operations are made available at the alternate processing site or if contracts are in place to support delivery to the site within an organization-defined time period for resumption.
controls provided at the alternate processing site are equivalent to those at the primary site.
the location or site of the facility where the system resides is planned considering physical and environmental hazards.
an alternate processing site is sufficiently separated from the primary processing site to reduce susceptibility to the same threats is identified.
potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster are identified.
explicit mitigation actions to address identified accessibility problems are outlined.
alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives) are developed.
the alternate processing site is prepared so that the site can serve as the operational site supporting essential mission and business functions.
circumstances that preclude returning to the primary processing site are planned for.
circumstances that preclude returning to the primary processing site are prepared for.
alternative communications protocols in support of maintaining continuity of operations are defined.
the capability to employ alternative communications protocols are provided in support of maintaining continuity of operations.
system operations to be resumed for essential mission and business functions are defined.
time period within which to resume essential mission and business functions when the primary telecommunications capabilities are unavailable is defined.
alternate telecommunications services, including necessary agreements to permit the resumption of system operations, are established for essential mission and business functions within an organization-defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services are obtained.
primary telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives) are developed.
alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives) are developed.
Telecommunications Service Priority is requested for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.
alternate telecommunications services from providers that are separated from primary service providers are obtained to reduce susceptibility to the same threats.
the frequency at which to obtain evidence of contingency testing by providers is defined.
the frequency at which to obtain evidence of contingency training by providers is defined.
primary telecommunications service providers are required to have contingency plans.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

the confidentiality of backup sensitive / regulated data is protected at storage locations.
system components for which to conduct backups of user-level information are defined.
the frequency at which to conduct backups of user-level information consistent with recovery time and recovery point objectives is defined.
the frequency at which to conduct backups of system-level information consistent with recovery time and recovery point objectives is defined.
the frequency at which to conduct backups of system documentation consistent with recovery time and recovery point objectives is defined.
backups of user-level information contained in system components are conducted frequently.
backups of system-level information contained in the system are conducted frequently.
backups of system documentation, including security- and privacy-related documentation are conducted frequently.
the confidentiality of backup information is protected.
the integrity of backup information is protected.
the availability of backup information is protected.
the frequency at which to test backup information for media reliability is defined.
the frequency at which to test backup information for information integrity is defined.
backup information is tested frequently to verify media reliability.
backup information is tested frequently to verify information integrity.
critical system software and other security-related information backups to be stored in a separate facility are defined.
backup copies of critical system software and other security-related information are stored in a separate facility or in a fire rated container that is not collocated with the operational system.
assets are reimaged from configuration-controlled images.
images are integrity-protected that represent a secure, operational state.
the confidentiality of backup sensitive / regulated data is protected at storage locations.
backup information to protect against unauthorized disclosure and modification is defined.
cryptographic mechanisms are implemented to prevent unauthorized disclosure and modification of backup information.
a sample of backup information in the restoration of selected system functions is used as part of contingency plan testing.
time period consistent with recovery time and recovery point objectives is defined.
transfer rate consistent with recovery time and recovery point objectives is defined.
system backup information is transferred to the alternate storage site for an organization-defined time period.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

dual authorization for the deletion or destruction of backup information is enforced.
Role Based Access Controls (RBAC) are utilized to logically restrict access to backups to privileged users with assigned roles for data backup and recovery operations.
Physical Access Controls (PAC) are utilized to physically restrict access to backups to privileged users with assigned roles for data backup and recovery operations.
Role Based Access Controls (RBAC) are utilized to logically restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles.
secure baseline configurations exist for systems, applications and/or services protect the confidentiality and integrity of data being stored, processed and/or transmitted.
systems, applications and/or services are securely recovered / reconstituted to a known, trusted state after a disruption, compromise or failure.
transaction recovery is implemented for systems that are transaction-based.
system components for which Mean Time to Failure (MTTF) should be determined are defined.
Mean Time to Failure (MTTF) substitution criteria to be used as a means to exchange active and standby components are defined.
Mean Time to Failure (MTTF) is determined for system components in specific environments of operation.
substitute system components and a means to exchange active and standby components are provided in accordance with Mean Time to Failure (MTTF) substitution criteria.
electronic discovery (eDiscovery) capabilities cover current and archived communication transactions.
restoration time period within which to restore system components to a known, operational state is defined.
the capability to restore system components within organization-defined restoration time periods from configuration-controlled and integrity-protected information representing a known, operational state for the components is provided.
system components used for recovery and reconstitution are protected.
the organization utilizes an isolated, non-production environment to perform data backups via offline, cloud or off-site capabilities.
the organization utilizes an isolated, non-production environment to perform recovery operations through offline, cloud or off-site capabilities.
an inventory of systems and system components that are required for critical business functions to operate exists.
Mean Time Between Failure (MTBF) is defined for systems and system components that are required for critical business functions.
Recovery Time Objectives (RTOs) are defined for systems and system components that are required for critical business functions.
Recovery Point Objectives (RPOs) are defined for systems and system components that are required for critical business functions.
systems and system components that are or may be hard to replace in a supply chain disruption are identified.
resources are allocated to obtain hard to replace identified systems and system components for critical business functions.
a pool of hard to replace identified systems and system components for critical business functions is maintained.
an incident handling capability for incidents involving Artificial Intelligence (AI) and Autonomous Technologies (AAT) exists.
processes are in place to handle failures or incidents in third-party data or Artificial Intelligence (AI) and Autonomous Technologies (AAT) deemed to be high-risk.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

the effects of types of denial-of-service events are organizationally-defined.
controls by type of denial-of-service event are employed to achieve the denial-of-service protection objective.
capacity planning is conducted so that the necessary capacity exists during contingency operations for information processing.
capacity planning is conducted so that the necessary capacity exists during contingency operations for telecommunications.
capacity planning is conducted so that the necessary capacity exists during contingency operations for environmental support.
the operating state and health status of critical systems is centrally-monitored.
the operating state and health status of critical applications is centrally-monitored.
the operating state and health status of services is centrally-monitored.
the time period to retain records of configuration-controlled changes is defined.
the configuration change control element responsible for coordinating and overseeing change control activities is defined.
the frequency at which the configuration control element convenes is defined.
configuration change conditions that prompt the configuration control element to convene are defined.
the types of changes to the system that are configuration-controlled are determined and documented.
proposed configuration-controlled changes to the system are reviewed.
proposed configuration-controlled changes to the system are approved or disapproved with explicit consideration for cybersecurity & privacy impact analyses.
configuration change decisions associated with the system are documented.
approved configuration-controlled changes to the system are implemented.
records of configuration-controlled changes to the system are retained for organization-defined time period.
activities associated with configuration-controlled changes to the system are monitored.
activities associated with configuration-controlled changes to the system are reviewed.
configuration change control activities are coordinated and overseen by organization-defined configuration change control element.
the configuration control element convenes organization-defined criteria.
changes to the system are tracked.
changes to the system are reviewed.
changes to the system are approved or disapproved.
changes to the system are logged.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

organization-defined time period.
organization-defined automated mechanisms are used to prohibit changes to the system until designated approvals are received.
organization-defined automated mechanisms are used to document all changes to the system.
organization-defined automated mechanisms are used to notify organization-defined personnel when approved changes to the system are completed.
changes to the system are tested before finalizing the implementation of the changes.
changes to the system are validated before finalizing the implementation of the changes.
changes to the system are documented before finalizing the implementation of the changes.
the frequency at which changes are to be reviewed is defined.
the circumstances under which changes are to be reviewed are defined.
changes to the system are reviewed organization-defined frequency or when organization-defined circumstances to determine whether unauthorized changes have occurred.
systems or system components that implement the security design principle of secure system modification are defined.
systems or system components implement the security design principle of secure system modification.
security representatives required to be members of the change control element are defined.
privacy representatives required to be members of the change control element are defined.
the configuration change control element of which the cybersecurity & privacy representatives are to be members is defined.
organization-defined security representatives are required to be members of the organization-defined configuration change control element.
organization-defined privacy representatives are required to be members of the organization-defined configuration change control element.
security responses to be automatically implemented are defined.
organization-defined security responses are automatically implemented if baseline configurations are changed in an unauthorized manner.
automated mechanisms place misconfigured or unauthorized system components in a quarantine or remediation network.
automated mechanisms to detect misconfigured or unauthorized system components are identified.
automated mechanisms are employed to detect misconfigured or unauthorized system components.
misconfigured or unauthorized system components are detected.
after detection, system components are removed and/or placed in a quarantine or remediation network to facilitate patching, re-configuration or other mitigations.
controls provided by cryptographic mechanisms that are to be under configuration management are defined.
cryptographic mechanisms used to provide organization-defined controls are under configuration management.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

physical access restrictions associated with changes to the system are defined and documented.
physical access restrictions associated with changes to the system are approved.
physical access restrictions associated with changes to the system are enforced.
mechanisms used to automate the enforcement of access restrictions are defined.
access restrictions for change are enforced using organization-defined automated mechanisms.
audit records of enforcement actions are automatically generated.
software components requiring verification of a digitally signed certificate before installation are defined.
firmware components requiring verification of a digitally signed certificate before installation are defined.
the installation of software components is prevented unless it is verified that the software has been digitally signed using a certificate recognized and approved by the organization.
the installation of firmware components is prevented unless it is verified that the firmware has been digitally signed using a certificate recognized and approved by the organization.
software or firmware components to be authenticated by cryptographic mechanisms prior to installation are defined.
cryptographic mechanisms are implemented to authenticate software or firmware components prior to installation.
critical or sensitive system and organizational operations for which dual authorization is to be enforced are identified.
dual authorization is employed to execute critical or sensitive system and organizational operations.
frequency at which to review privileges is defined.
frequency at which to reevaluate privileges is defined.
privileges to change system components within a production or operational environment are limited.
privileges to change system-related information within a production or operational environment are limited.
privileges are reviewed organization-defined frequency.
privileges are reevaluated organization-defined frequency.
privileges to change software resident within software libraries are limited.
as part of the organization's change management processes, stakeholders are alerted to spread awareness of the potential impact(s) from proposed changes.
security functions to be verified for correct operation are defined.
privacy functions to be verified for correct operation are defined.
system transitional states requiring the verification of cybersecurity & privacy functions are defined.
frequency at which to verify the correct operation of cybersecurity & privacy functions is defined.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

the results of security and/or function verification are reported to pertinent personnel or roles.
secure baseline configurations exist for cloud-based systems, applications and services to protect the confidentiality, integrity and availability of data being stored, processed and/or transmitted.
the organization facilitates the implementation of cloud management controls to ensure cloud instances are securely configured and maintained.
the design and configuration process for cloud services is formally governed so systems, applications and processes are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.
the decommission process for cloud services is formally governed so that data is securely transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.
a cloud security architecture is defined to address cloud employments that support the organization's mission.
the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.
cloud security management subnets are logically isolated.
cloud security management subnet system components and functions to be isolated are defined.
organization-defined criteria are used to isolate cloud security management subnets.
information processing interoperability is supported.
information/data exchange supports secure data portability.
virtual machine images are protected to ensure continued integrity.
virtual machine images are governed according to the organization's established change control processes.
multi-tenant owned / managed assets (physical and virtual) are designed and governed such that provider and customer (tenant) user access is appropriately segmented from other tenant users.
a documented Customer Responsibility Matrix (CRM) delineates assigned responsibilities for controls between the Cloud Service Provider (CSP) and its customers.
for Multi-Tenant Service Providers (MTSP), established security event logging capabilities for its customers are consistent with the customer's applicable statutory, regulatory and/or contractual obligations.
for Multi-Tenant Service Providers (MTSP), there is a capability to conduct prompt forensic investigations in the event of a suspected or confirmed security incident.
for Multi-Tenant Service Providers (MTSP), there is a capability to conduct prompt response to suspected or confirmed security incidents and vulnerabilities, including timely notification to affected customers.
cloud providers use secure protocols for information/data exchange to support secure data portability.
cloud providers use industry-recognized formats to support secure interoperability.
cloud providers provide documentation of custom changes to virtualization formats for review by affected stakeholders.
locations where information processing and data storage is/are to be restricted are defined.
requirements or conditions for restricting the location of information processing, information storage or information services are defined.
based on requirements, information processing, information storage or information services is/are restricted to locations.
the geographic location of information processing and data storage is restricted to facilities located within the legal jurisdictional boundary of the United States.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

instances of non-compliance with statutory, regulatory and/or contractual obligations are documented, including the reason(s) for non-compliance.
instances of non-compliance with statutory, regulatory and/or contractual obligations are formally-reviewed.
instances of non-compliance with statutory, regulatory and/or contractual obligations are centrally-governed to maintain appropriate situational awareness.
instances of non-compliance with statutory, regulatory and/or contractual obligations are assigned to individuals or teams for remediation.
remediation plans for instances of non-compliance with statutory, regulatory and/or contractual obligations are documented.
the organization's applicable cybersecurity and privacy controls are determined through the analysis of business practices to determine required statutory, regulatory and/or contractual compliance obligations.
a recurring process exists to validate the scope of cybersecurity and privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.
a continuous monitoring strategy is developed for cybersecurity & privacy controls.
continuous control monitoring is implemented in accordance with the organization's continuous monitoring strategy.
the frequency of security and/or privacy control assessments is defined.
security and/or privacy controls are assessed with the defined frequency to determine if the controls are effective in their application.
security and/or privacy controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.
personnel or roles to whom the security and/or privacy status of the system is reported are defined.
frequency at which the security and/or privacy status of the system is reported is defined.
system-level continuous monitoring includes reporting the cybersecurity & privacy status of the system to pertinent personnel or roles according to an organization-defined frequency.
control monitoring metrics are defined.
system-level continuous monitoring includes ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy.
system-level continuous monitoring includes correlation and analysis of information generated by control assessments and monitoring.
system-level continuous monitoring includes response actions to address the results of the analysis of control assessment and monitoring information.
the personnel or roles for reporting the security status of organizational systems to is/are defined.
the personnel or roles for reporting the privacy status of organizational systems to is/are defined.
the frequency at which to report the security status of organizational systems is defined.
the frequency at which to report the privacy status of organizational systems is defined.
an organization-wide continuous monitoring strategy is developed.
continuous monitoring programs are implemented that include establishing metrics to be monitored.
continuous monitoring programs are implemented that establish frequency for monitoring.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

continuous monitoring programs are implemented that include reporting the security status of organizational systems to personnel or roles frequency.
continuous monitoring programs are implemented that include reporting the privacy status of organizational systems to personnel or roles frequency.
an internal audit function exists that is comprised of stakeholders who have the subject matter expertise to serve in an advisory capability on audit-related matters.
an internal audit function formally defines audit-related priorities for the organization.
an internal audit function tracks audit findings that require remediation efforts.
an internal audit function provides the organization's executive leadership with insights into the appropriateness of the organization's technology and information governance processes.
the frequency at which to assess controls in the system and its environment of operation is defined.
individuals or roles to whom control assessment results are to be provided are defined.
an appropriate assessor or assessment team is selected for the type of assessment to be conducted.
a control assessment plan is developed that describes the scope of the assessment, including controls and control enhancements under assessment.
a control assessment plan is developed that describes the scope of the assessment, including assessment procedures to be used to determine control effectiveness.
a control assessment plan is developed that describes the scope of the assessment, including the assessment environment.
a control assessment plan is developed that describes the scope of the assessment, including the assessment team.
a control assessment plan is developed that describes the scope of the assessment, including assessment roles and responsibilities.
the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment.
independent assessors or assessment teams are employed to monitor in-scope controls on an ongoing basis.
controls are assessed in the system and its environment of operation assessment frequency to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting established security requirements.
controls are assessed in the system and its environment of operation assessment frequency to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting established privacy requirements.
a control assessment report is produced that documents the results of the assessment.
the results of the control assessment are provided to individuals or roles.
an internal audit function formally defines audit-related priorities for the organization.
audits are thoughtfully planned to minimize the impact of audit-related activities on business operations.
a formal process exists to intake requests, document the request and determine whether a government agency has an applicable and valid legal basis to request data from the organization.
based on an applicable and valid legal basis for a data request by a government agency, data request fulfillment actions are formally assigned to an individual or group with explicitly-specified criteria to minimize inappropriate data sharing.
a formal process exists to intake and document government investigation requests.
a formal process exists to evaluate government investigation requests for legal requirements the organization must comply with.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

executive leadership, along with legal counsel, formally identifies primary risks associated with compliance (e.g., loss of confidentiality and/or integrity considerations with data governance).
executive leadership, along with legal counsel, formally identifies secondary risks associated with compliance (e.g., non-compliance with other laws, regulations and contractual agreements).
executive leadership, along with legal counsel, formally identifies tertiary risks associated with compliance (e.g., human rights abuses, theft of intellectual property, espionage, etc.).
executive leadership, along with legal counsel, formally adopts an action plan to respond to host government requests for unrestricted and non-monitored access to the organization's systems, applications and services that could potentially violate other applicable statutory, regulatory and/or contractual obligations.
the scope for the configuration management plan is organization-wide.
the current configuration management policy is reviewed and updated organization-defined frequency.
the current configuration management policy is reviewed and updated following organization-defined events.
personnel or roles to review and approve the configuration management plan is/are defined.
a configuration management plan for the system is developed and documented.
a configuration management plan for the system is implemented.
the configuration management plan addresses roles.
the configuration management plan addresses responsibilities.
the configuration management plan addresses configuration management processes and procedures.
the configuration management plan establishes a process for identifying configuration items throughout the system development life cycle.
the configuration management plan establishes a process for managing the configuration of the configuration items.
the configuration management plan defines the configuration items for the system.
the configuration management plan places the configuration items under configuration management.
the configuration management plan is reviewed and approved by organization-defined personnel or roles.
the configuration management plan is protected from unauthorized disclosure.
the configuration management plan is protected from unauthorized modification.
the responsibility for developing the configuration management process is assigned to organizational personnel who are not directly involved in system development.
security configuration settings for information technology products employed in the system are established and included in the baseline configuration.
a current baseline configuration of the system, application or service is developed and documented.
the baseline configuration includes hardware, software, firmware and documentation.
the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle under configuration control.
security configuration settings for information technology products employed in the system are enforced.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives

the baseline configuration of the system is reviewed and updated organization-defined frequency.
the baseline configuration of the system is reviewed and updated when required due to organization-defined circumstances.
the baseline configuration of the system is reviewed and updated when system components are installed or upgraded.
system components for which to manage, apply and verify configuration settings are defined.
automated discovery and management tools for the inventory of system components are identified.
an up-to-date, complete, accurate and readily available inventory of system components exists.
automated discovery and management tools are employed to maintain an up-to-date, complete, accurate and readily available inventory of system components.
the number of previous baseline configuration versions to be retained is defined.
organization-defined number of previous baseline configuration version(s) of the system is/are retained to support rollback.
a baseline configuration for system development environments that is managed separately from the operational baseline configuration is maintained.
a baseline configuration for test environments that is managed separately from the operational baseline configuration is maintained.
the systems or system components to be issued when individuals travel to high-risk areas are defined.
configurations for systems or system components to be issued when individuals travel to high-risk areas are defined.
organization-defined systems or system components with organization-defined configurations are issued to individuals traveling to locations that the organization deems to be of significant risk.
organization-defined controls are applied to the systems or system components when the individuals return from travel.
network devices are configured to synchronize startup and running configuration files.
common secure configurations to establish and document configuration settings for components employed within the system are defined.
system components for which approval of deviations is needed are defined.
operational requirements necessitating approval of deviations are defined.
configuration settings that reflect the most restrictive mode consistent with operational requirements are established and documented for components employed within the system using common secure configurations.
any deviations from established configuration settings for system components are identified and documented based on operational requirements.
any deviations from established configuration settings for system components are approved.
changes to the configuration settings are monitored in accordance with organizational policies and procedures.
changes to the configuration settings are controlled in accordance with organizational policies and procedures.
actions to be taken upon an unauthorized change are defined.
configuration settings requiring action upon an unauthorized change are defined.

Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0)
Licensed by Creative Commons Attribution-NoDerivatives