SECURE CONTROLS FRAMEWORK

SCRMS

SECURITY, COMPLIANCE & RESILIENCE MANAGEMENT SYSTEM

A Framework & Technology-Agnostic Approach to Design, Implement and Maintain Secure, Compliant and Resilient Capabilities.

Version 2026.1

This publication is available free of charge from: https://securecontrolsframework.com/content/scrms.pdf

Table of Contents

1 FOREWORD

1.1 PURPOSE

Entities invest in cybersecurity and data protection as a necessity, driven in large part by statutory, regulatory and/or contractual requirements. To build and maintain efficient and effective operations, a cybersecurity and data protection program must have a hierarchical vision, mission and strategy that directly supports broader strategic objectives and business processes.

A Security, Compliance & Resilience Management System (SCRMS) is a framework and technology-agnostic approach to design, implement and maintain secure, compliant and resilient capabilities to cover an entity's People, Processes, Technology, Data and Facilities (PPTDF), regardless of how or where data is stored, processed and/or transmitted.

The SCRMS is a framework and technology-agnostic approach to cybersecurity and data protection controls to identify, implement and manage Secure, Compliant and Resilient (SCR) capabilities. This is designed to cover an entity's People, Processes, Technologies, Data and Facilities (PPTDF), regardless of how or where data is stored, processed and/or transmitted.

The underlying expectation is for those charged with developing, implementing and governing security, compliance and resilience capabilities to do so in a reasonable manner that would withstand scrutiny that could take the form as an external auditor, regulator or prosecuting attorney.

1.2 FRAMEWORK-AGNOSTIC APPROACH

By design, the SCRMS expands upon and modernizes the concept of traditional Information Security Management System (ISMS) models, due to the archaic nature of multiple, siloed "management systems" that are necessary to provide reasonable governance practices (e.g., Artificial Intelligence Management System (AIMS) add-on). The use of siloed ISMS, AIMS and similar stand-alone management systems fails to address the reality of modern business practices, since it is overly leveraged for marketing purposes. This does not serve assurance needs to demonstrate security, compliance or resilience that entities require. The SCRMS offers a broader "security, compliance and resilience ecosystem" mindset that is designed to provide the necessary coverage to address applicable risks and threats that entities face.

The SCRMS enables an entity to align with one, or more, laws, regulations and/or frameworks. For example, an entity that aligns with NIST CSF 2.0, but also has obligations for PCI DSS, ISO 27001, ISO 42001, HIPAA Security Rule and SOC 2 can leverage a "living control set" that is capable of adjusting to the specific security, compliance and resilience requirements it must address.

1.3 TARGET AUDIENCE

The SCRMS is written for senior cybersecurity practitioners and executives, specifically those in the following roles:

- Chief Information Security Officer (CISO); and
- Governance, Risk & Compliance (GRC) Director.

While any cybersecurity practitioner can benefit from the information provided in the SCRMS, those roles listed above are the primary decision-makers within an entity that enable a focus on secure, compliant and resilient practices. Their utilization of the SCRMS will trickle down to all other parts of the entity's cybersecurity and data protection program.

1.4 INTENT

The SCRMS is not a "one-size-fits-all" playbook, since the information in this document is meant to be adopted and tailored to the unique size, resources and risk circumstances of the entity. The SCRMS is:

- Framework-agnostic, allowing entities to leverage one or more frameworks that it needs to align with (e.g., NIST CSF 2.0, SOC 2, NIST 800-171, ISO 27001, etc.);
- Focused on supporting processes and practices that must exist for a cybersecurity and data protection program to operate effectively and efficiently;
- Designed to proactively address the strategic, operational and tactical nature of operating an entity's cybersecurity and data protection program; and
- Designed to address both internal controls, as well as the broader concept of Cybersecurity Supply Chain Risk Management (C-SCRM).

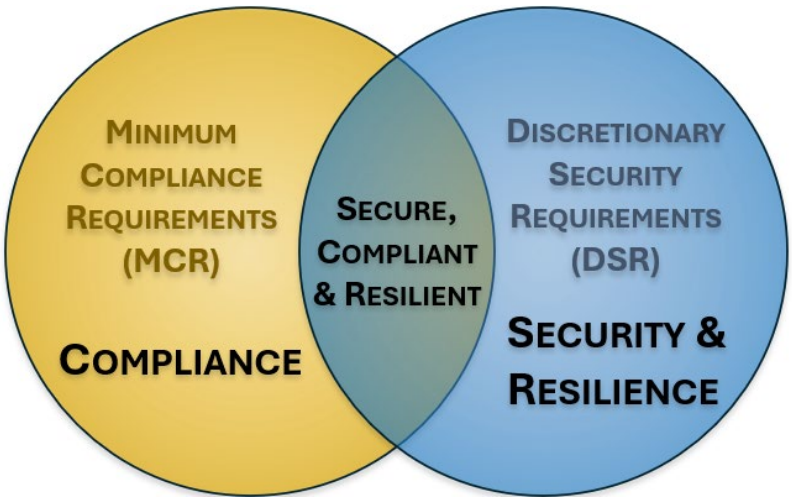
This document can help an entity understand the variables the make-up the *"Who? What? When? Where? How? and Why?"* questions that arise when designing, implementing and maintaining secure, compliant and resilient capabilities.

1.5 RISK-BASED GOVERNANCE PRACTICES

Secure, compliant and resilient capabilities exist when applicable controls are properly scoped and implemented. The SCRMS specifically addresses the need to clarify the difference between "compliant" versus "secure" since that understanding is necessary to have coherent risk management discussions.

To assist in this process, an entity's applicable controls are categorized according to "must have" vs "nice to have" requirements:

- Minimum Compliance Requirements (MCR) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts (e.g., mandatory requirements). MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- Discretionary Security Requirements (DSR) are tied to the entity's risk appetite since DSR are "above and beyond" MCR, where the entity self-identifies additional cybersecurity and data protection controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments (e.g., discretionary requirements). DSR are primarily internally-influenced, based on the entity's respective industry and risk tolerance. While MCR establish the foundational floor that must be adhered to, DSR are where entities often achieve improved efficiency, automation and enhanced security.



The combination of MCR and DSR equate to an entity's Minimum Security Requirements (MSR), which define the "must have" and "nice to have" requirements in one control set. This control set defines the Minimum Viable Product (MVP) technical and business requirements from a cybersecurity and data protection perspective. The MSR can be considered to be an entity's IT General Controls (ITGC), which establish the necessary controls that must be applied to applicable Technology Assets, Applications, Services and/or Data (TAASD).

1.6 Integrated Controls Management (ICM) – Controls Centric Mindset

The SCRMS is controls-centric, where controls are viewed as the nexus, or central pivoting point, for an entity's cybersecurity and data protection operations. This affects the entity's overall business rhythm, since the controls used to define "secure practices" have both direct and indirect impacts on the TAASD that business operations rely upon.

The graphic helps visualize the controls-centric nature of the SCRMS:

- Policies are enforced by standards, which map to controls.
- Procedures are "control activities" that describe the formal processes in place to operationalize a control.
- Metrics (including analytics) are tied to control execution.
- Threat catalogs should map threats to controls, since threats affect control execution.
- Risk catalogs should map risk to controls, since risks exist from control deficiencies and/or absences.
- Evidence artifacts provide evidence of due diligence and due care that controls operate.
- Assessment Objectives (AOs) are tied to controls to provide objective criteria to determine control implementation and operation.

1.7 Understanding Risks vs Threats

With the understanding that controls are the nexus of a cybersecurity and data protection program. To progress from identifying an entity's specific MCR and DSR to making a determination of risks and threats, it is important to baseline the understanding of risk and threat management terminology.

1.7.1 Risk Determination

A risk is:

- *noun*: A situation where someone, or something valued, is exposed to danger, harm or loss; or
- *verb*: To expose someone or something valued to danger, harm or loss.

In order to determine if something is a risk, address it as a question of, ***"Does the issue / event being assessed relate to either (1) the existence of or (2) a deficiency with an existing control (e.g., safeguard)?"***

- If it does, the entity may be exposed to one, or more, risks.
- Those risks are expected to be documented in a risk catalog that is specific to the entity.

If the issue / event being assessed does not relate to either (1) the existence of or (2) a deficiency with an existing control, then it may be a threat.

1.7.2 Threat Determination

A threat:

- *noun*: Is a person, or thing, likely to cause damage or danger; or
- *verb*: Indicates impending damage or danger.

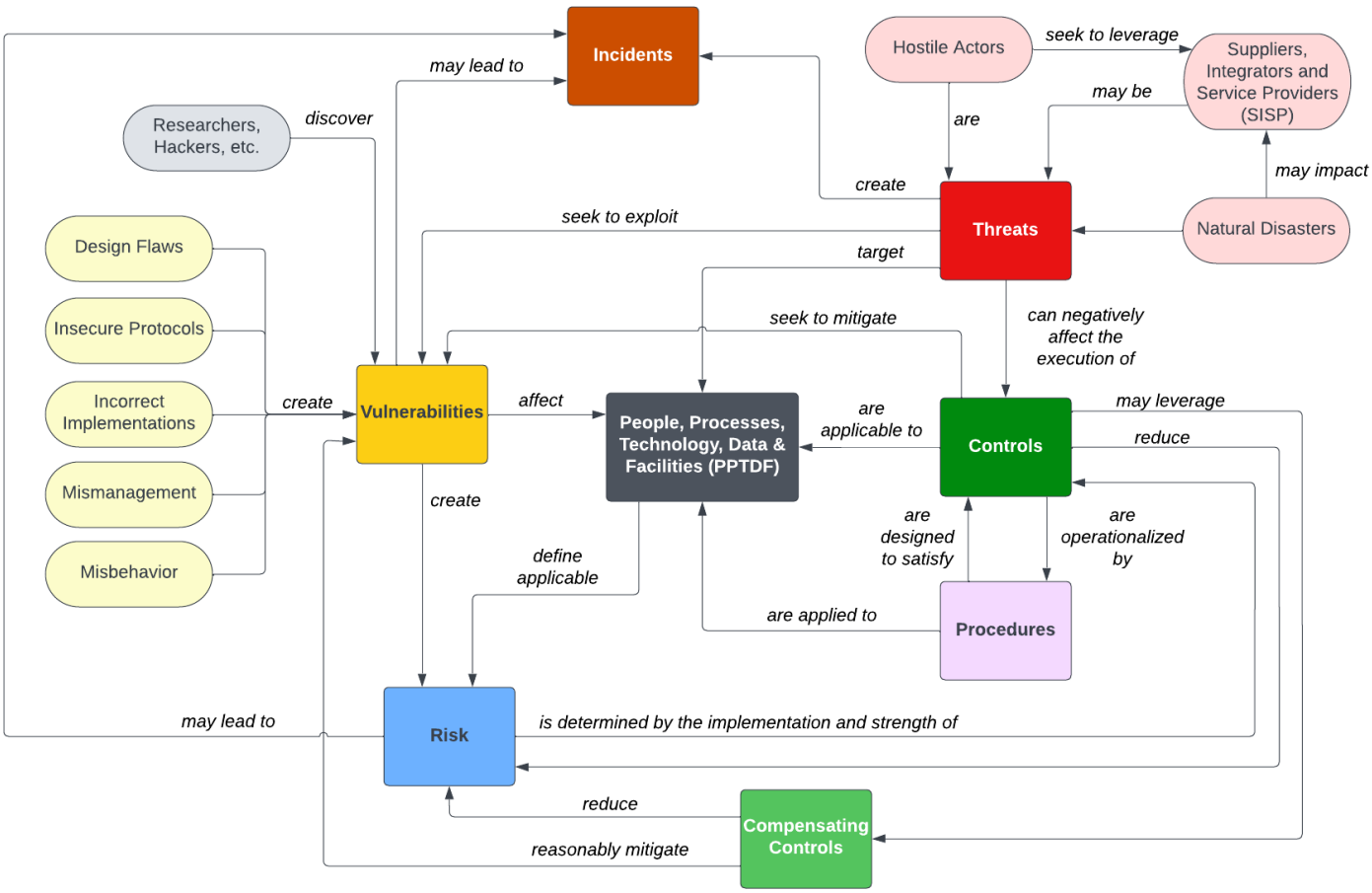
In order to determine if something is a threat, address it as a question of ***"Does the issue / event being assessed affect control execution (e.g., the ability of the safeguard to function as intended)?"***

- If it does, the entity may be exposed to one, or more, threats; and
- Those threats are expected to be documented in a threat catalog that is specific to the entity. Ideally, the threats are broken down into natural and man-made threats.

1.7.3 Risk vs Threat Ecosystem – Path To Better Communications

Risk, threat and vulnerability management practices are meant to achieve a minimum level of protection that equates to a reduction in the total risk due to the safeguards an entity implements via controls. From an ecosystem perspective, the many

components have unique meanings that need to be understood to reasonably protect PPTDF. Understanding the context of how these components integrate can lead to more meaningful communications and practical risk management practices:[1]



1.8 PROHIBITIONS

The following usages of this content are strictly prohibited:

(1) Use without proper attribution to the SCF Council;
(2) Creating derivative works based on this content;
(3) Training Artificial Intelligence (AI) technologies; and/or
(4) Use as part of an AI dataset or any other AI-related activities.

1.9 LIABILITY LIMITATIONS

THIS CONTENT IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE CONTENT OR THE USE OR OTHER DEALINGS IN THE CONTENT.

[1] *ComplianceForge Risk vs Threat vs Vulnerability Ecosystem - https://complianceforge.com/free-guides/threat-vs-vulnerability-vs-risk*

2 NORMATIVE REFERENCES

SCF Council Guidance
A normative reference is a reference document that is considered to be essential and indispensable to establish foundational practices.

Without the following normative reference(s) being utilized, the entity's Security Compliance & Resilience Management System (SCRMS) is unlikely to be fully or correctly implemented:

(1) Secure Controls Framework (SCF);
(2) Unified Scoping Guide (USG);
(3) Security, Compliance & Resilience Risk Management Model (SCR-RMM);
(4) Security, Compliance & Resilience Capability Maturity Model (SCR-CMM); and
(5) Cybersecurity & Data Protection Assessment Standards (CDPAS).

3 TERMINOLOGY STANDARDIZATION

From the context of applying a standard to the Security Compliance & Resilience Management System (SCRMS), it is important to clarify mandatory versus optional criteria:[2]

- The terms "*SHALL*" and "*SHALL NOT*" indicate requirements:
  - To be followed strictly in order to conform; and
  - From which no deviation is permitted.
- The terms "*SHOULD*" and "*SHOULD NOT*" indicate that:
  - Among several possibilities, one (1) is recommended as particularly suitable, without mentioning or excluding others;
  - A certain course of action is preferred, but not necessarily required; or
  - A certain possibility, or course of action, is discouraged, but not prohibited.
- The terms "MAY" and "NEED NOT" indicate a course of action permissible within reasonable limits.
- The terms "*CAN*" and "*CANNOT*" indicate:
  - A possibility and capability; or
  - The absence of that possibility or capability.

3.1 AUTHORITATIVE SOURCES

The SCF Council recognizes two (2) primary sources for authoritative definitions for cybersecurity and data protection terminology:

(1) The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define cybersecurity-related terminology;[3] and

(2) NIST Glossary.[4]

3.2 DEFINITIONS

Within the cybersecurity profession, the term "control" can be applied to a variety of contexts and can serve multiple purposes. When used in the SCRMS context, a control is a mechanism (e.g., a safeguard or countermeasure) designed to address protection needs specified by an entity's requirements.

- Controls are:
  - The power to make decisions about how something is managed or how something is done;
  - The ability to direct the actions of someone or something;
  - An action, method or law that limits; and/or
  - A device or mechanism used to regulate or guide the operation of a machine, apparatus or system.
- Requirements are statements that translate, or express, a need and its associated constraints and conditions.

Additional clarification for assessment-relevant terminology:

- Assessment Boundary. The scope of an entity's control implementation to which assessment of objects is applied:
  - An assessment may involve multiple assessment boundaries; and
  - Assessment boundary may be defined as the People, Processes, Technologies, Data and/or Facilities (PPTDF) that comprise:
    - The entire entity;
    - A specific contract, project or initiative;
    - A specific Business Unit (BU) within an entity; or
    - A specific country, or geographic region, of the entity's business operations.
- Assessment Object. The item (e.g., specifications, mechanisms, activities, individuals) upon which an assessment method is applied during an assessment.
- Assurance. Grounds for justified confidence that a security or privacy claim has been or will be achieved. [5]
- Conformity Assessment. A demonstration that specified requirements are fulfilled.

[2] *NIST SP 800-63A - https://pages.nist.gov/800-63-3/sp800-63a.html*
[3] *NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf*
[4] *NIST Glossary - https://csrc.nist.gov/glossary*
[5] *NIST Glossary for Assurance - https://csrc.nist.gov/glossary/term/assurance*

- Control Inheritance: Security control inheritance is a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized and monitored by entities other than those responsible for the system or application; entities either internal or external to the entity where the system or application resides. [6]
- Due Care. The standard of care where a reasonable person would exercise in the same situation or under similar circumstances. This standard of care is used in a tort action to determine whether a person was negligent.[7]
- Due Diligence. The level of reasonable care or attention expected to avoid liability. [8]
- Implemented Capability. An implemented capability is a technical, administrative or physical mechanism that exists in a production environment and can demonstrate reasonable effectiveness.
- Loss. A negative impact from an incident that can be categorized as:
    - Productivity loss;
    - Data loss;
    - Financial loss; and/or
    - Reputation loss.
- Material Control. When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. A material control is such a fundamental cybersecurity and/or data protection control that:
    - It is not capable of having compensating controls; and
    - Its absence, or failure, exposes an entity to such a degree that it could have a material impact.
- Material Risk. When an identified risk that poses a material impact, that is a material risk.
    - A material risk is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.); and
    - A material risk should be identified and documented in an entity's "risk catalog" that chronicles the entity's relevant and plausible risks.
- Material Threat. When an identified threat poses a material impact, that is a material threat.
    - A material threat is a vector that has the potential to cause damage or danger that results in a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and
    - A material threat should be identified and documented in an entity's "threat catalog" that chronicles the entity's relevant and plausible threats.
- Material Incident. When an incident poses a material impact, that is a material incident.
    - A material incident is an occurrence that does or has the potential to:
        - Jeopardize the Confidentiality, Integrity, Availability and/or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits with a material impact on the entity; and/or
        - Constitute a violation, or imminent threat of violation, of an entity's policies, standards, procedures or acceptable use practices that has a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.).
    - Reasonably foreseeable material incidents should be documented in an entity's Incident Response Plan (IRP) that chronicles the entity's relevant and plausible incidents, so there are appropriate practices to identify, respond to and recover from such incidents.
- Material Weakness. A material weakness is a deficiency, in an entity's cybersecurity and/or data protection controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the entity can adhere to its stated risk tolerance.
    - When there is an existing deficiency (e.g., control deficiency) that poses a material impact, that is a material weakness (e.g., inability to maintain access control, lack of situational awareness to enable timely identification and response to incidents, etc.).
    - A material weakness will be identified as part of a gap assessment, audit or other form of assessment as a finding due to one (1), or more, control deficiencies. A material weakness should be documented in an entity's Plan of Action & Milestones (POA&M), risk register, or similar tracking mechanism for remediation purposes.

[6] *NIST Glossary for Security Control Inheritance - https://csrc.nist.gov/glossary/term/security_control_inheritance*
[7] *Cornell Law School Legal Information Institute - https://www.law.cornell.edu/wex/due_care*
[8] *Cornell Law School Legal Information Institute - https://www.law.cornell.edu/wex/due_diligence*

- Mechanism. A mechanism can be described as a: [9]
  - Process or system that is used to produce a particular result; or
  - Device or method for achieving a security-relevant purpose.
- Reciprocity. Reciprocity is an agreement among participating entities to accept each other's: [10]
  - Security assessments to reuse system resources; and/or
  - Assessed security posture to share information.
- Risk. A risk is:
  - A situation where someone, or something valued, is exposed to danger, harm or loss (noun); or
  - To expose someone or something valued to danger, harm or loss (verb).
- Risk Appetite: The types and amount of risk, on a broad level, an entity is willing to accept in its pursuit of value. [11]
- Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a desired result. [12]
- Risk Threshold: Values used to establish concrete decision points and operational control limits to trigger management action and response escalation. [13]
- Threat. A threat:
  - Is a person, or thing, likely to cause damage or danger (noun); or
  - Indicates impending damage or danger (verb).
- Trust. A belief that an entity meets certain expectations and therefore, can be relied upon. [14]

3.3 ACRONYMS

The following acronyms are used throughout the SCRMS:

Acronym	Term	Definition
1PD	First Party Declaration	1PDs are self-attestations (e.g., internal assessments).
3PA	Third-Party Attestation	3PA are attestations made by an independent third-party, generally in the performance of an assessment or audit.
3PAAC	Third-Party Assessment, Attestation and Certification Services	Assessment, attestation and certification services performed by a third-party entity.
3PAO	Third-Party Assessment Entity	A company that performs assessment, attestation and certification services.
AAT	Artificial Intelligence and Autonomous Technologies	Tools that are advanced enough to act with limited human involvement through Artificial Intelligence (AI), Machine Learning (ML) or similar autonomous technologies.
AI	Artificial Intelligence	AI is software that AI mimics human cognitive functions (e.g., thinking, learning and creativity).
AO	Assessment Objective	AOs are objective statements that establish the desired outcome for the assessment for a specific control. There may be multiple AOs associated with a control.
CIAS	Confidentiality, Integrity, Availability and/or Safety	CIAS is an evolution of the "CIA Triad" concept that defines the purpose of security controls. It adds the component of Safety.
COI	Conflict of Interest	COI involves situations in which a personal interest, or relationship, conflicts with the faithful performance of an official duty.
CPE	Continuing Professional Education	CPE describes the ongoing process of improving skills and competencies through formal or informal educational activities.
CPS	Cyber-Physical Systems	CPS are a form of OT. OT integrate computing resources to control physical devices. CPS act as a bridge between the physical and digital world.

[9] *NIST Glossary for Mechanism - https://csrc.nist.gov/glossary/term/mechanism*
[10] *NIST Glossary for Reciprocity - https://csrc.nist.gov/glossary/term/reciprocity*
[11] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*
[12] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*
[13] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*
[14] *NIST Glossary for Trust - https://csrc.nist.gov/glossary/term/trust*

CSP	Cloud Service Provider	An external entity providing on-demand network access to shared, configurable computing resources such as networks, servers and storage (e.g., PaaS, IaaS, SaaS, etc.).
DSR	Discretionary Security Requirements	DSR are discretionary cybersecurity and/or data protection controls that address voluntary industry practices or internal requirements. DSR are primarily internally influenced, based on the entity's respective industry and risk tolerance.
ERL	Evidence Request List	ERLs establish a finite list of supporting evidence used in an assessment: ▪ Prior to the start of the assessment, an ERL is provided by the 3PAO to the OSA. ▪ The ERL's standardized evidence expectations allow OSAs to have sufficient time to accumulate reasonable evidence to determine the adequacy of control design and operation.
ESP	External Service Provider	An independent, third-party entity that provides services, technologies, facilities and/or people. ESPs include but are not limited to: ▪ Consulting / professional services; ▪ Software development; ▪ Staff augmentation; and ▪ Technology support (e.g., Managed Services Provider (MSP)).
HMI	Human-Machine Interface	HMI consists of software and/or interfaces that monitors and/or sends commands to controllers within an ICS.
IaaS	Infrastructure as a Service	IaaS is a cloud computing model that delivers on-demand, virtualized computing resources (e.g., servers, storage, networking, etc.). The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).
IC	Implemented Capability	IC refer to technical, administrative and physical controls where: ▪ Technology capabilities will only be considered implemented if the system(s), application(s) and/or service(s) has/have been operational in a production environment for at least sixty (60) days; ▪ Administrative processes will only be considered implemented if there is evidence to demonstrate that process has been: o Used in a real-world situation (e.g., onboarding/offboarding personnel, incident response, etc.); and/or o Formally tested (e.g., documented incident response exercise); and ▪ Physical capabilities will only be considered implemented if the physical security mechanism(s) has/have been operational in a production environment for at least thirty (30) days.
ICS	Industrial Control Systems	ICS are a type of OT. An ICS is broader system of technologies that includes PLCs, sensors and networks.
IoT	Internet of Things	IoT refers to Internet-enabled technologies (e.g., smart devices) that can provide monitoring and automation tasks.
MCR	Minimum Compliance Requirements	MCR are minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations.
ML	Machine Learning	ML is a subset of AI that enables systems to earn from large data sets to identify patterns and make predictions without being explicitly programmed for every specific task.
MLC	Maturity Level Criteria	MLC are specific to each maturity level to define reasonable staffing, technologies and processes to implement the desired level of maturity.
MSA	Master Services Agreement	MSAs are comprehensive contracts between two parties that establish terms and conditions of current and future transactions.
OT	Operational Technology	OT encompasses systems that detect and/or cause direct changes in the physical world by monitoring and controlling assets and processes (e.g., industrial technologies).

PaaS	Platform as a Service	IaaS is a cloud computing model that provides pre-configured tools, databases and middleware as a platform that enables consumers to build, deploy and manage applications. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
PbD	Privacy by Design	Data privacy through the design and governance of processes and technologies. PbD prioritizes data protection as a core business requirement, rather than a technical feature.
PLC	Programmable Logic Controller	PLCs are a type of IT. PLCs are "ruggedized" technologies that are designed for industrial settings to automate manufacturing processes, machineries and/or industrial systems.
RASCI	Responsible, Accountable, Supportive, Consulted & Informed	Refers to a RASCI matrix that defines responsibilities associated with individuals or teams: ▪ Responsible - entity directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - entity overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - entity(ies) under the coordination of the Responsible person for support in performing the task; ▪ Consulted - entity(ies) not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - entity(ies) not involved in task execution but are informed when the task is completed.
ROC	Report on Conformity	A formalized report that issues an assessment conformity designation. The ROC summarizes the assessment findings and justification for the conformity designation.
SaaS	Software as a Service	SaaS is a cloud computing model that offers software and/or services on a subscription bases, accessed over the Internet.
SbD	Secure by Design	Processes and technologies are designed and built in a way that protects against reasonable threats. SbD prioritizes cybersecurity as a core business requirement, rather than treating it as a technical feature.
SCADA	Supervisory Control and Data Acquisition	SCADA is a type of OT. It is a Human-Machine Interface (HMI) for operators to monitor, control and adjust physical industrial processes in real-time.
SCR	Security, Compliance & Resilience	Refers to the three (3) key components of the Security, Compliance & Resilience Management System (SCRMS).
SOW	Statement of Work	SOWs are contracts that cover the work management aspects of a project (e.g., scope, timeline, cost, responsibilities, etc.).

4 INTRODUCTION

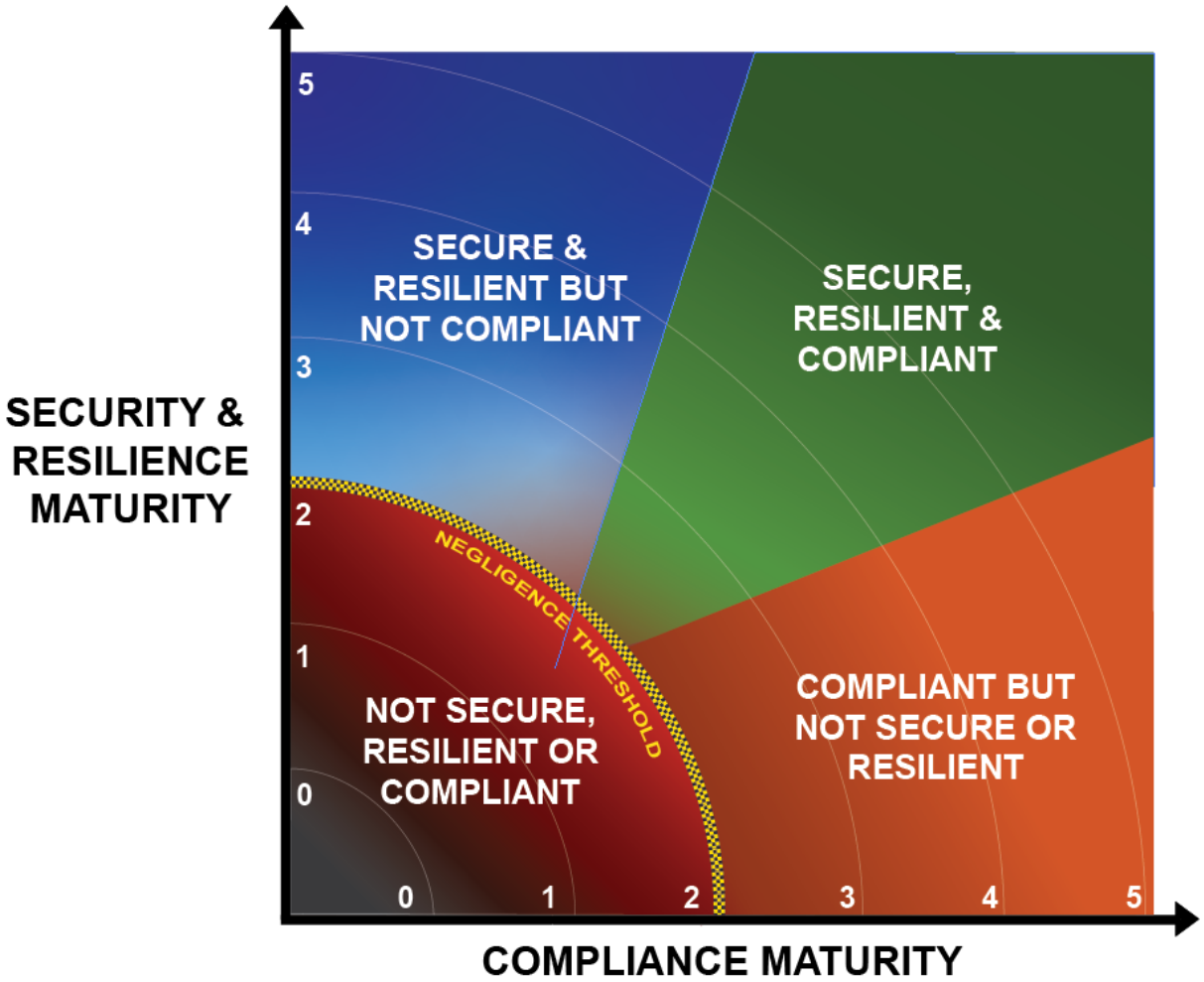
There are two (2) fundamental goals of the Security, Compliance & Resilience Management System (SCRMS):

(1) Provide the structure for an entity to be secure, compliant and resilient; and
(2) Generate defensible evidence of due diligence and due care that is capable of defending the entity's cybersecurity and data protection practices to against legal challenges, if an incident should occur.

This defensibility is anchored in the Living Control Set (LCS), which converts governance intent into defined, prioritized and testable control expectations.

An entity's status can be visualized as being in one (1) of four (4) maturity-based quadrants where that entity is either:

(1) Not secure, resilient or compliant (negligent);
(2) Secure & resilient, but not compliant;
(3) Compliant, but not secure or resilient; or
(4) Secure, resilient & compliant.



This concept of identifying a negligence threshold is addressed in the SCF's Security, Compliance & Resilience Capability Maturity Model (SCR-CMM).[15]

[15] *SCF SCR-CMM - https://securecontrolsframework.com/capability-maturity-model/*

4.1 Defensible Evidence

Artifacts must be adequate and sufficient. Defensible evidence is documented evidence that is so well-collected and preserved that the adequacy and sufficiency of those artifacts are:

- Irrefutable, where its authenticity and integrity make the artifacts admissible in court or formal proceedings; and
- Capable of withstanding legal challenges (e.g., auditor, regulator, class action lawsuit, etc.).

Defensible evidence:

- Should be viewed as the "natural byproduct" of secure, compliant and resilient practices, where this evidence can be leveraged to support a claim or argument effectively because its origin(s) and handling are standardized and legally sound; and
- Must demonstrate conformity with the entity's LCS, including validation of material controls and documented risk decisions.

4.2 Understanding Security vs Compliance vs Resilience

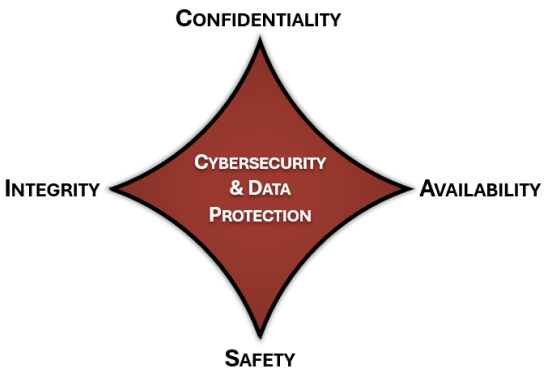
The terms security, compliance and resilience are unique, where each has its own specific meaning.

4.2.1 What Does It Mean To Be Secure?

An entity can reasonably claim it is secure if it has implemented and operational defenses focused on Confidentiality, Integrity, Availability and Safety (CIAS). An entity's level of security is dynamic, based on its:

(1) Implemented defensive capabilities; and
(2) Applicable risks and threats.

Effective security requires a unified effort involving those that interact with the entity's Technology Assets, Applications, Services and/or Data (TAASD). Commensurate with applicable risk and threats, cybersecurity and data protection measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of TAASD. This also includes protection against accidental loss or destruction. The protection of TAASD must include safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:



- **Confidentiality** addresses preserving authorized restrictions on access and disclosure to authorized users and services, including means for protecting personal data privacy and proprietary information.
- **Integrity** addresses protecting against improper modification or destruction, including ensuring non-repudiation and authenticity.
- **Availability** addresses timely, reliable access to data, systems and services for authorized users, services and processes.
- **Safety** addresses reducing risk associated with technologies that could fail or be manipulated by nefarious actors to cause death, injury, illness, damage to or loss of equipment.

4.2.2 What Does It Mean To Be Compliant?

An entity can reasonably claim it is compliant if it has the ability to demonstrate conformity with applicable laws, regulations and other obligations. The scope of compliance includes both external and internal requirements.

4.2.3 What Does It Mean To Be Resilient?

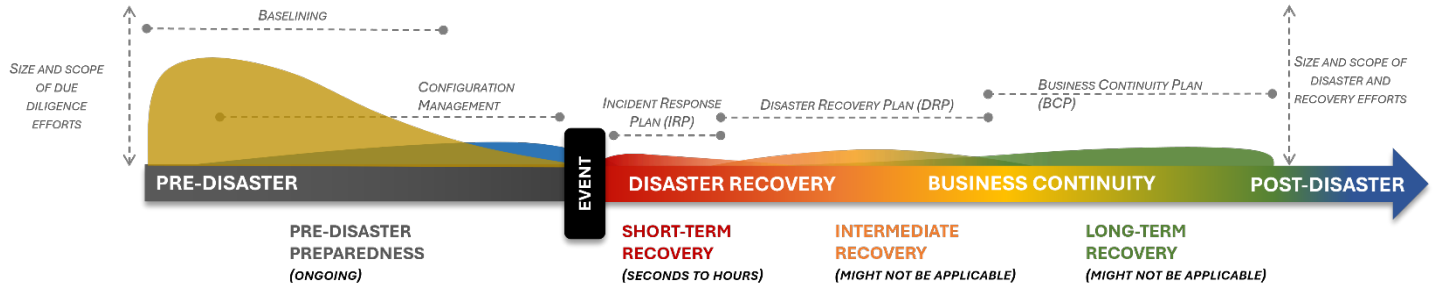
An entity can reasonably claim it is resilient if it has prepared for and has the ability to adapt to changing conditions, where it can withstand and/or recover rapidly from disruption.

Resilience includes the ability to withstand and recover from deliberate attacks, accidents or naturally occurring threats or incidents.[16]

[16] *NIST Glossary for Resilience - https://csrc.nist.gov/glossary/term/resilience*

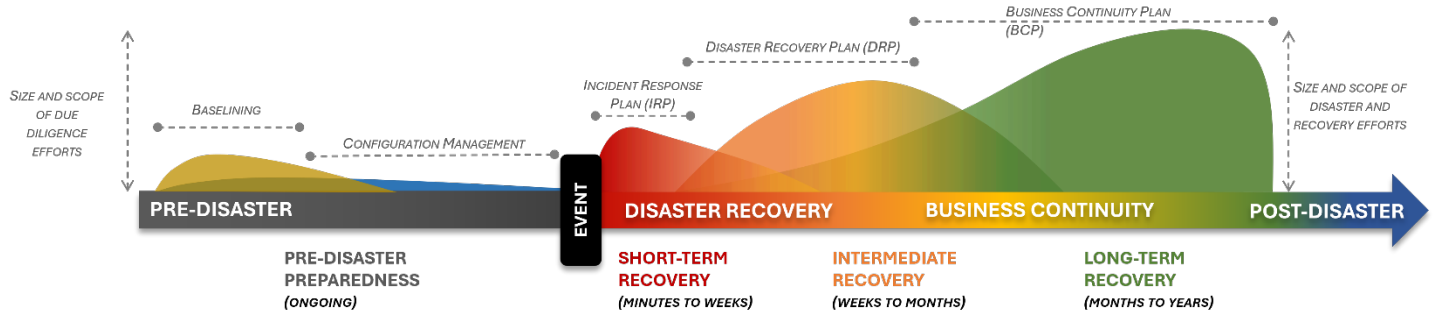
4.2.3.1 *Pre-Event Focus*

An entity that focuses on "left of event," or pre-event preparedness, indicates a commitment to resiliency, based on its ability to minimize negative business impacts from reasonably anticipated incidents and/or threats.



4.2.3.2 *Post-Event Focus*

An entity that focuses on "right of event," or post-event preparedness, indicates a lack of commitment to resiliency, based on the forecast difficulties and length of duration the business will experience operational impacts. Recovery planning by itself does not equate to resiliency, since the business interruptions during the recovery phase may be insurmountable if not tied to business uptime requirements (e.g., meet Service Level Agreements (SLAs), customer satisfaction goals, etc.).



4.3 Defining Negligence As It Pertains To Security, Compliance & Resilience Practices

The following content is leveraged from Cornell's Law School Legal Information Institute (LII)[17] to provide context on the concept of negligence.

Negligent conduct may consist of either an act or an omission to act when there is a duty to do so. Primary factors to consider in ascertaining whether the person's conduct lacks reasonable care are:

- The foreseeable likelihood that the person's conduct will result in harm;
- The foreseeable severity of any harm that may ensue; and
- The burden of precautions to eliminate or reduce the risk of harm.

Four (4) elements are generally required to establish a *prima facie* case of negligence:

(1) Existence of a legal duty that the defendant owed to the plaintiff.
Example: A requirement to comply with NIST SP 800-171 to protect Controlled Unclassified Information (CUI) as part of a contract.

(2) Defendant's breach of that duty.
Example: A failure to protect CUI in accordance with NIST SP 800-171 requirements under applicable DFARS clauses.

(3) Plaintiff's sufferance of an injury.
Example: Financial losses due to fines and/or lost contracts stemming from non-compliance with DFARS clauses.

(4) Proof that defendant's breach caused the injury.
Example: A whistleblower claims, forensic investigations and/or publicity about the data breach or other evidence pointing to the entity being the source of the data breach.

[17] *Cornell's Law School - https://www.law.cornell.edu/wex/negligence*

Typically, to meet the injury element of the *prima facie* case, the injury must be one (1) of two (2) things:

(1) Bodily harm; and/or
(2) Harm to property (can be personal property or business property (physical or digital)).

4.3.1 Determining A Breach Of Duty

In determining whether the defendant has breached a duty, courts may use the *Learned Hand Formula*[18], which is an algebraic approach to determining liability. If $B < PL$, then there will be negligence liability for the party with the burden of taking precautions where:

- B = Burden of taking precautions
- P = Probability of loss
- L = Gravity of loss

If the burden of taking such precautions is less than the probability of injury multiplied by the gravity of any resulting injury, then the party with the burden of taking precautions will have some amount of liability.

4.3.2 Determining Whether There Was A Duty To Act

Typically, if the defendant had a duty to act, did not act (resulting in a breach of duty) and that breach of duty caused an injury, then the defendant's actions will be classified as misfeasance. There are several ways to determine whether the defendant had a duty to act:

- The defendant engaged in the creation of the risk which resulted in the plaintiff's harm;
- The defendant volunteered to protect the plaintiff from harm;
- The defendant knew / should have known that the conduct will harm the plaintiff; or
- Business/voluntary relationships.

[18] *Learned Hand Formula* - https://academic.oup.com/lpr/article/5/1/1/990799

5 SCOPE OF SECURITY, COMPLIANCE & RESILIENCE ACTIVITIES

An entity's Security Compliance & Resilience Management System (SCRMS) is designed to address a Plan, Do, Check and Act (PDCA) approach for continuous improvements that span development, implementation, maintenance and remediation activities.

SCF Council Guidance

Scoping is an activity that spans both due diligence and due care. The concept of "gaming" the scope of an assessment or accreditation boundary to minimize the deployment of reasonable controls for the sake of obtaining a certification is disingenuous and borders on fraud when that audit or certification is used to market the security, compliance and/or resilience capabilities of an entity. Activities that alter the scope of controls for the perceived benefit of the entity create a potential material misrepresentation of risk.

From a SCRMS perspective, the goal is for compliance to be a natural byproduct of secure and resilient capabilities, so entities should focus on secure engineering and data protection principles to guide the development, implementation and operation of its cybersecurity and data protection program.

5.1 SCOPE DETERMINATION

The scope of the SCRMS encompasses:

- The entity, as a whole (e.g., business units, departments, geographies, personnel, etc.); and
- Any entity that directly or indirectly affects the security, compliance and/or resilience of the entity.

Entities that have the potential to directly or indirectly affect security, compliance and/or resilience capabilities include:

- Cloud Service Providers (CSPs) are external entities that provide on-demand network access to shared, configurable computing resources such as networks, servers and storage (e.g., Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS)).
- External Service Providers (ESPs) include, but are not limited to:
    - Software as a Service (SaaS) solutions include, but are not limited to:
        - Managed Service Provider (MSP) that includes but is not limited to the following managed Information Technology (IT) services:
            - Helpdesk;
            - Remote data backups;
            - Network administration; and
            - System maintenance.
        - Managed Security Services Provider (MSSP) include but are not limited to the following cybersecurity services:
            - Threat detection and analytics;
            - Vulnerability assessments; and
            - Incident response.
        - Human Resources (HR) augmentation, including but not limited to:
            - Timesheets;
            - Personnel management;
            - Recruitment;
            - Benefits management; and
            - Payroll.
        - Business operations augmentation, including but not limited to:
            - Managed phone systems;
            - Facilities management automation;
    - Delivering supplementing resources where a third-party provides skills or capacity that is lacking by the entity. This includes, but is not limited to:
        - Staff augmentation;

- Specialized expertise (e.g., consultants);
- Software development;
- Marketing agency support;
- Facilities maintenance services;
- Legal services;
- Financial services; and
- Colocation facilities (COLO); and

- Material suppliers include, but are not limited to:
  - Raw materials; and
  - Components needed for products and/or services.

SCF Council Guidance

The difference between a CSP and ESP can sometimes be nuanced. Following the stringent definitions set forth by the US Department of Defense, the SCRMS adopts the following interpretation:[19]

CSP means an external company that provides cloud services based on cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

An ESP would be considered a CSP when it provides its own cloud services based on a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing that can be rapidly provisioned and released with minimal management effort or service provider interaction.

An ESP would not be considered a CSP when it provides technical support services to its clients. It would be considered a Managed Service Provider (MSP) or Managed Security Services Provider (MSSP) where:

(1) It does not host its own cloud platform offering;
(2) It may utilize cloud offerings to deliver services to clients without being a CSP; and
(3) An ESP that manages a third-party cloud service on behalf of a client would not be considered a CSP.

5.2 CONTROL APPLICABILITY

Cybersecurity practitioners generally agree that the importance of robust cybersecurity and data protection controls cannot be overstated. However, the applicability of those controls is sometimes in question since not all controls are applicable. To help demonstrate the applicable nature of controls:

- An employee cannot have a secure baseline configuration applied.
- An Incident Response Plan (IRP) cannot sign a Non-Disclosure Agreement (NDA), use Multi-Factor Authentication (MFA) or be patched.
- An entity cannot apply end user training to a firewall.
- Sensitive and/or regulated data cannot be assigned roles and responsibilities.
- A data center cannot undergo employee background screening.

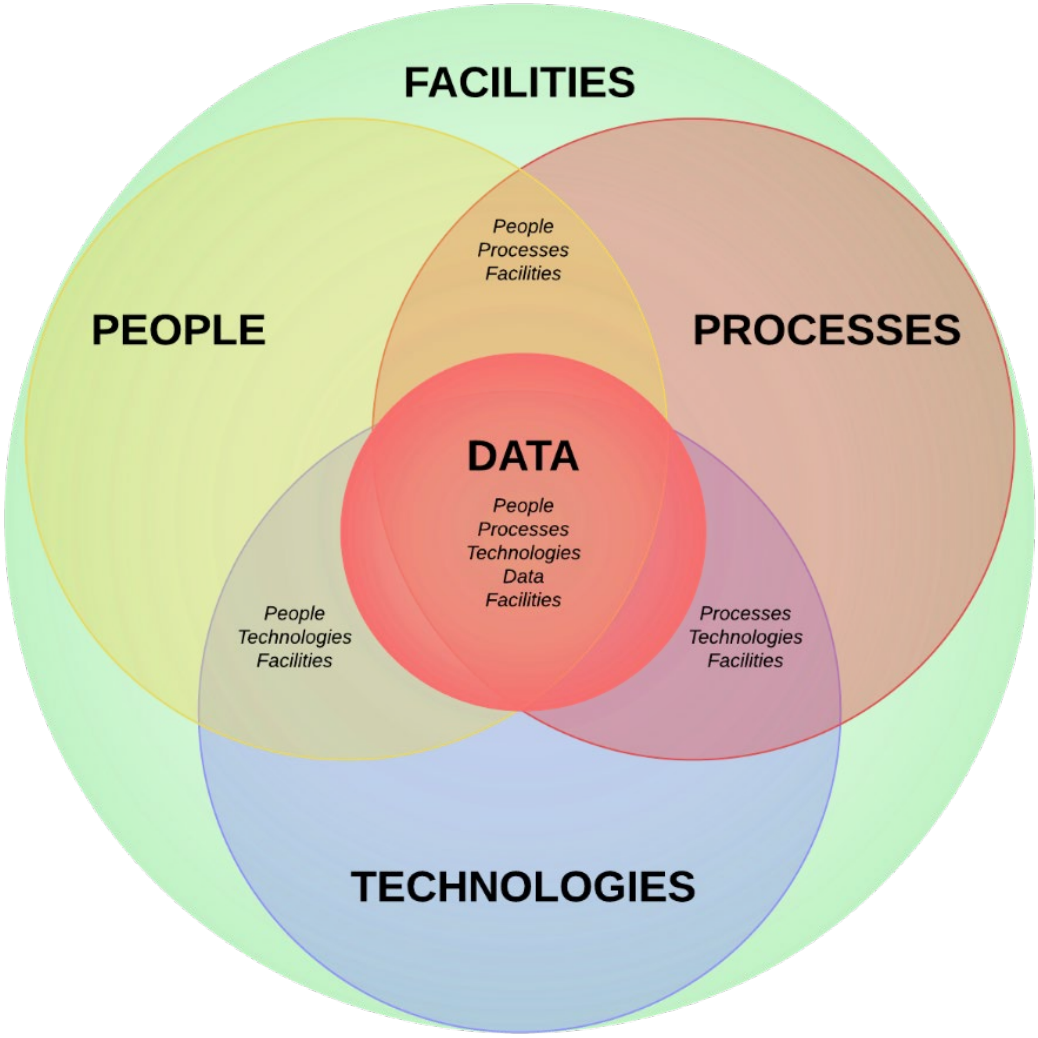
NOTE: Applicability determinations directly affect inclusion within the Living Control Set (LCS) and therefore must be formally documented.

[19] *US DoD CMMC Resources & Documentation - https://dodcio.defense.gov/cmmc/Resources-Documentation/*

5.3 People, Processes, Technology, Data & Facilities (PPTDF)

The People, Processes, Technology, Data and Facilities (PPTDF) model provides a comprehensive approach to address control applicability. These five (5) components provide a lens to view the applicability of controls:

1. People. Control directly applies to humans (e.g., training, background checks, non-disclosure agreements, etc.).
2. Processes. Control directly applies to administrative work performed (e.g., processes, procedures, administrative documentation, etc.).
3. Technologies. Control directly applies to systems, applications and services (e.g., secure baseline configurations, patching, etc.).
4. Data. Control directly applies to data protection (e.g., encrypting sensitive and/or regulated data, applying metatags, etc.).
5. Facilities. Control directly applies to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).



6 SECURITY, COMPLIANCE & RESILIENCE MANAGEMENT SYSTEM (SCRMS) PRINCIPLES

An entity's cybersecurity program becomes defensible when evidence exists to prove:

(1) Risks were identified;
(2) Controls were recommended; and
(3) Leadership made informed decisions.

This methodical approach creates a legally defensible paper trail. The principles of the SCRMS can help an entity create and maintain this defensible evidence. The following Annexes provide CISO-focused guidance on this topic:

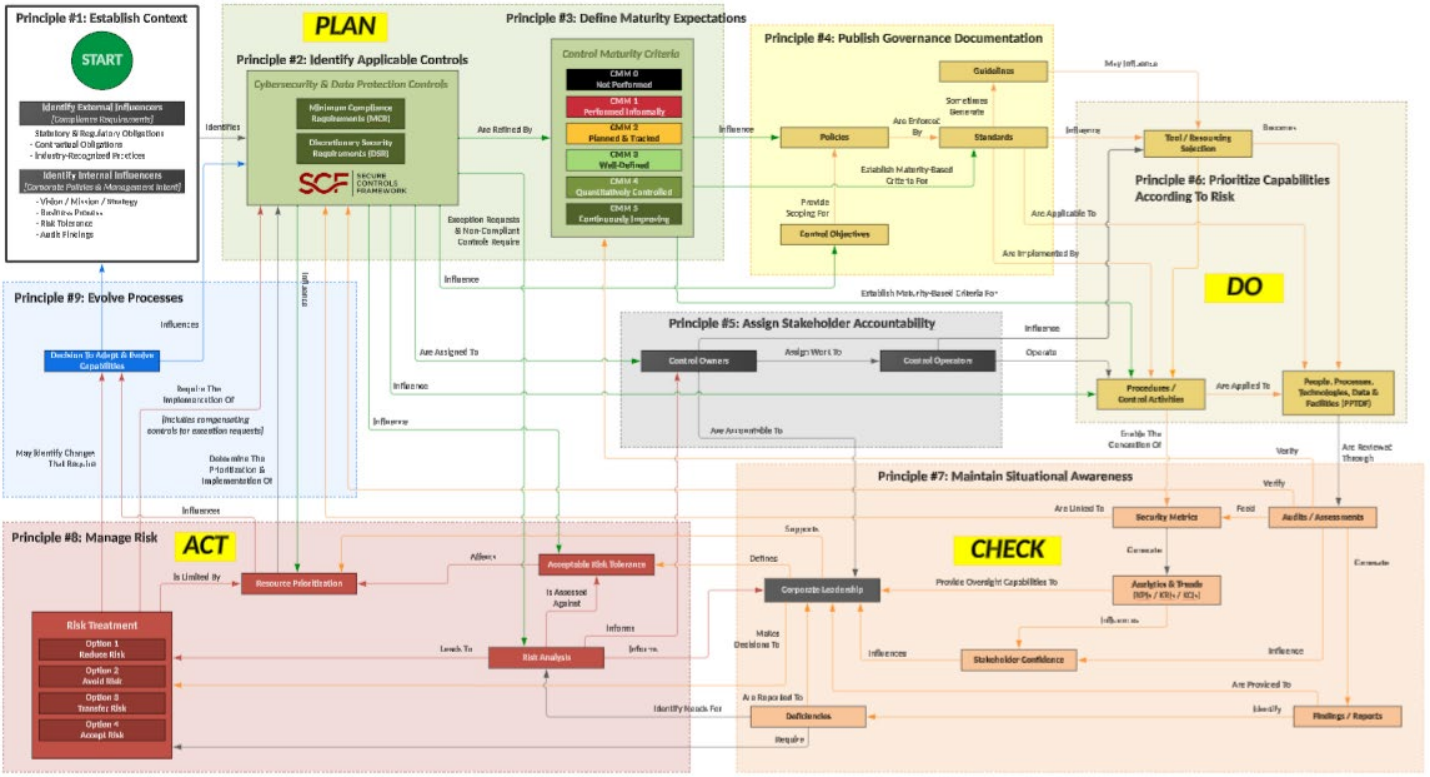
- Annex 3: Defensible Evidence; and
- Annex 4: Planning For Resistance.

6.1 SCRMS PRINCIPLES

There are nine (9) principles associated with the Security, Compliance & Resilience Management System (SCRMS):

(1) Establish Context
(2) Identify Applicable Controls
(3) Define Maturity Expectations
(4) Publish Governance Documentation
(5) Assign Stakeholder Accountability
(6) Prioritize Capabilities According To Risk
(7) Maintain Situational Awareness
(8) Manage Risk
(9) Evolve Processes

NOTE: Principle #2 is where the Living Control Set (LCS) is established. As processes evolve and require adjustment, the LCS should be updated in Principle #9.



[graphic download - https://securecontrolsframework.com/content/plan-do-check-act.pdf]

6.2 SCRMS Principle 1: Establish Context

To build and maintain efficient and effective operations, a cybersecurity and data protection program must have a hierarchical vision, mission and strategy that directly supports the entity's broader strategic objectives and business processes. This process of establishing context involves identifying all applicable external compliance requirements (e.g., laws, regulations and contractual obligations), internal directives (e.g., Board of Directors, corporate policies, etc.). This also includes understanding applicable risks and threats, since the entity's exposure to those may influence the need for controls beyond those that are mandated as compliance obligations.

Establishing context is both a due diligence and due care element of an entity's cybersecurity and data protection program, since context changes with time. Things to consider when establishing context:

- Mission / vision / strategy of the entity;
- Statutory (law), regulatory (regulation) and contractual requirements for cybersecurity and data protection;
- Fiscal constraints;
- The entity's structure;
- The entity's risk profile (including risk appetite, risk tolerance and risk threshold considerations);
- Planned entity changes (e.g., Mergers, Acquisitions & Divestitures (MA&D));
- Corporate culture (e.g., how receptive is the entity to change); and
- Geographic-specific requirements.

SCF Council Guidance

Part of an entity's due diligence activities involve establishing the context for the SCRMS. Practical steps to establish context for the SCRMS include talking with representatives outside of IT and cybersecurity to document the following information:

(1) The entity's structure:
- *a. Reporting structure (e.g., chain of command);*
- *b. IT / cybersecurity governance stakeholders;*
- *c. Supply chain partners; and*
- *d. Geographic locations;*

(2) The entity's:
- *a. Mission;*
- *b. Vision; and*
- *c. Strategy;*

(3) Risk management practices:
- *a. Risk tolerance;*
- *b. Risk appetite; and*
- *c. Risk thresholds; and*

(4) Constraints that affect business operations:
- *a. Applicable legal obligations:*
  - *i. Statutory (law);*
  - *ii. Regulatory (regulation); and*
  - *iii. Contractual requirements;*
- *b. Fiscal constraints; and*
- *c. Corporate culture (e.g., how receptive the entity is to change).*

6.3 SCRMS Principle 2: Identify Applicable Controls

A tailored set of cybersecurity and data protection controls must exist for an entity to implement a SCRMS. This control set needs to be tailored for the entity's unique requirements, such as a combination of Minimum Compliance Requirements (MCR) and Discretionary Security Requirements (DSR). This blend of "must have" and "nice to have" requirements establish an entity's tailored control set to help ensure secure, compliant and resilient capabilities.

SCF Council Guidance

Part of an entity's due diligence process is to identify applicable cybersecurity and data protection controls. Practical steps to identify applicable controls include:

(1) Reading through the Secure Controls Framework (SCF) principles to become familiar with the thirty-three (33) domains to understand how they come together to address the security, compliance and resilience considerations for a modern cybersecurity and data protection program.

(2) As "business enablers," CISOs should talk with representatives outside of IT and cybersecurity to gain an understanding of the entity's complete scope of compliance requirements (e.g., legal, procurement, physical security, etc.).

(3) Developing a list of the "must have" laws, regulations and frameworks that the entity must comply with.

(4) Developing a list of "nice to have" requirements that the entity's Board of Directors, or other stakeholders, feel are necessary.

Understanding the requirements for both cybersecurity and data protection principles involves a simple process of distilling expectations. This process is all part of documenting reasonable expectations that are "right-sized" for an entity, since every entity has unique requirements.

There is no expectation for an entity to utilize all 1,400+ controls in the SCF catalog. It is best to visualize the SCF as a "buffet of cybersecurity and data protection controls," where the entity only selects those controls necessary to address its unique requirements. Once the entity knows what is applicable, it is possible to use the SCF to generate a customized control set that is specific to address the entity's MCR and DSR.

Things to consider when defining applicable controls:

- *Controls to address "must have" requirements from laws, regulations and contractual obligations to ensure the entity is compliant with its obligations;*
- *Controls to address "discretionary" requirements that exist to ensure the entity has secure and resilient operations; and*
- *There needs to be at least an annual review to ensure the applicable controls are accurate to the current needs for compliance, security and resilience.*

6.4 SCRMS Principle 3: Define Maturity Expectations

The entity must define maturity expectations for its cybersecurity and data protection controls. From the perspective of the SCRMS, the maturity expectations define entity-specific "what right looks like" expectations for control implementation and continued operation. The maturity-based criteria are applicable to People, Processes, Technologies, Data & Facilities (PPTDF).

Maturity targets are expected to directly support the entity's need for security, compliance and resiliency capabilities. These maturity targets can be used by an entity's leadership for:

(1) Multi-year business planning;
(2) Budgeting; and
(3) Assessment criteria.

SCF Council Guidance

The SCF uses the Security, Compliance & Resilience Capability Maturity Model (SCR-CMM) criteria for each control. The SCR-CMM is an available option for maturity expectations for entities that lack maturity targets.

The SCR-CMM draws upon the high-level structure of the Systems Security Engineering Capability Maturity Model v2.0 (SSE-CMM), where it can be used to demonstrate varying levels of maturity for PPTDF at a control level.

Things to consider when assigning maturity-based criteria:

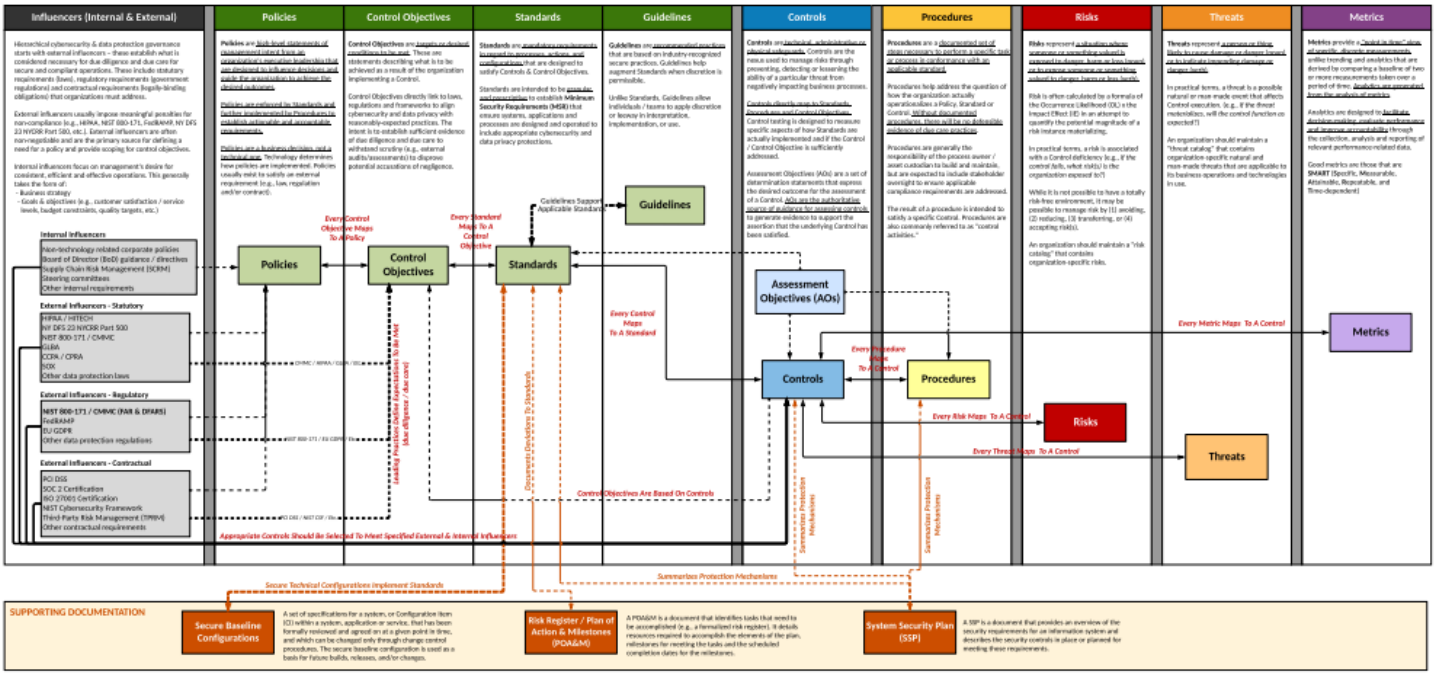
- *Not all controls need to be the same level of maturity, since each control has an associated cost. The higher the level of maturity, the higher the cost. This is a risk management decision to define what right looks like for the entity;*
- *The expected level of maturity needs to at least comply with applicable statutory, regulatory and contractual requirements; and*
- *Lower levels of maturity may be considered negligent behavior from a due care perspective.*

6.5 SCRMS Principle 4: Publish Governance Documentation

Cybersecurity and data protection documentation must exist, otherwise an entity's governance practices are both unenforceable and indefensible. Formalizing entity-specific requirements via documented policies, standards and procedures are necessary to operationalize cybersecurity and data protection controls.

Documented policies, standards and procedures provide evidence of due diligence that the entity identified and implemented reasonable steps to address its applicable requirements. The output of procedures provides evidence of due care that controls were operated as described.

Note: For governance practices, a reference model should be used to encourage clear communication by defining generally accepted cybersecurity and data protection documentation components and how those are linked. This can provide a comprehensive understanding of primary documentation components that are necessary to demonstrate evidence of due diligence and due care. As a reference, the Hierarchical Cybersecurity Governance Framework (HCGF) addresses the interconnectivity of key cybersecurity documentation components. [20]



SCF Council Guidance

There are generally three (3) options to generate cybersecurity and data protection documentation:

(1) Use internal resources to write it in-house;

(2) Hire a consultant to write a bespoke set of documentation; or

(3) Purchase semi-customized templates online.

[20] *ComplianceForge Hierarchical Cybersecurity Governance Framework (HCGF) - https://complianceforge.com/grc/hierarchical-cybersecurity-governance-framework/*

Things to consider when publishing policies & standards:

- *Departments other than cybersecurity and data privacy publish policies, standards and procedures (e.g., HR, IT, Procurement, Legal, etc.) and those need to be reconciled to ensure interoperability.*
- *The policies and standards need to reflect both the "must have" and "nice to have" requirements identified in SCRMS Principle 2;*
- *Policies are designed as "high level statements of management intent" and are not expected to change often;*
- *Standards should be designed to assign granular requirements to enforce policies. As technologies change/evolve, those standards must be reviewed and updated, as necessary, to ensure secure, compliant and resilient capabilities; and*
- *Procedures should be written at a level of detail that makes it repeatable through clear steps, but should avoid unnecessary content that makes the procedures too difficult to maintain. As business processes or technologies change, procedures must be updated to reflect the new method(s) necessary to operate a control.*

6.6 SCRMS Principle 5: Assign Stakeholder Accountability

Controls must be assigned to stakeholders to ensure accountability (e.g., business units, teams and/or individuals). These "control owners" are expected to assign the task of executing controls to "control operators" at the Individual Contributors (IC)-level.

- Stakeholders utilize the prescriptive requirements from policies and standards to develop Standardized Operating Procedures (SOP) that enable ICs to execute those controls.
- The documented execution of procedures provides evidence of due care that reasonable practices are being performed.

SCF Council Guidance

Assigning stakeholder accountability offers unique challenges for entities, since it is beyond IT, cybersecurity and data protection. Common stakeholders involve Human Resources (HR), procurement, facilities management, legal and many other teams to ensure accountability is enforceable. Realistically, this step is an executive-management function since it requires inter-departmental enforcement by an entity's management.

Things to consider when assigning stakeholder accountability:

- *Procedures are not "owned" by the cybersecurity or privacy teams. Procedures are the responsibility of the control owner / operator; and*
- *The NIST SP 800-181, Workforce Framework for Cybersecurity (NICE Framework), is a methodology to identify cybersecurity and data protection-related roles and associated responsibilities.[21] The NICE Framework offers an efficient way to assign stakeholder accountability for internal and external stakeholders.*

6.7 SCRMS Principle 6: Prioritize Capabilities According To Risk

Security, compliance and resilience capabilities must be prioritized based on applicable risks and threats. Not all risks and threats are equal, so a risk-based prioritization must occur.

SCF Council Guidance

Prioritization should be based on a CISO-level business plan that supports the entity's broader mission and strategy. That department-level business plan would reasonably be a multi-year approach to address security,

[21] *NIST SP 800-181 - https://csrc.nist.gov/pubs/sp/800/181/r1/final*

compliance and resilience capabilities. That formalized plan is used for resource allocation (e.g., staffing, technology purchases, service contracts, etc.) based on approval from the entity's executive leadership.

Things to consider when prioritizing capabilities:

- *Resources are finite, so a prioritized plan is expected to be spread out across multiple years; and*
- *The entity's executive leadership is expected to approve the prioritized plan, where the decision for the approved Course of Action (CoA) is elevated above the CISO role.*

6.8 SCRMS Principle 7: Maintain Situational Awareness

Situational awareness must involve more than merely "monitoring controls" (e.g., metrics). While metrics are a point-in-time snapshot into discrete controls performance, the broader view of metrics leads to a longer-term trend analysis (e.g., analytics). When properly tied in with current audits, control deficiencies, risk, threat and vulnerability information, this broader insight provides "situational awareness" that is necessary for an entity's leadership to adjust plans to operate within the defined risk threshold.

SCF Council Guidance

Things to consider when maintaining situation awareness:

- *Metrics/analytics tell the long-term story of how the cybersecurity and data protection program is doing. This historical performance provides context to an entity's senior leaders for decision-making purposes; and*
- *The metrics/analytics need to be tied to measurable controls that can help eliminate Fear, Uncertainty and Doubt (FUD) reporting.*

Maintaining situational awareness has different meanings, based on the security culture of an entity. Metrics / analytics reporting is often plagued by the problem of Garbage In, Garbage Out (GIGO). Often, the GIGO issue is rooted in an entity's executive leadership trying to explain their perceived needs for metrics to cybersecurity practitioners in a way that describes the design of a "football bat" (e.g., nonsensical solution). To combat GIGO, it is advisable to approach the problem from the perspective that executive management often just wants a simple answer to a relatively-straightforward question: "Are we secure?" The metrics and analytics should be able to answer that question with irrefutable evidence.

6.9 SCRMS Principle 8: Manage Risk

Proactive risk management processes must exist across all phases of Technology Assets, Applications, Services and/or Data (TAASD) life cycles to address Confidentiality, Integrity, Availability and Safety (CIAS) aspects. Based on finite resources (e.g., time, personnel and money), it is necessary to utilize prioritized risk management practices that ensure issues posing the highest risk are addressed first.

Risk management must address internal and external factors, including data privacy, Artificial Intelligence (AI), embedded technology and Supply Chain Risk Management (SCRM) considerations. To manage risk, it requires the entity to enforce a clearly-defined risk threshold and ensure reasonable security practices are operational.

SCF Council Guidance

Risk management involves coordinated activities that optimize the management of potential opportunities and adverse effects. Proactive risk management activities provide a way to realize potential opportunities without exposing an entity to unnecessary peril.

The goal of risk analysis is to determine the potential negative implications of an action or situation to determine one (1) of two (2) decisions:

(1) Acceptable Risk: the criteria fall within a range of acceptable parameters; or

(2) *Unacceptable Risk: The criteria fall outside a range of acceptable parameters.*

Traditional risk management practices have four (4) options to address identified risk:

(1) *Reduce the risk to an acceptable level;*
(2) *Avoid the risk;*
(3) *Transfer the risk to another party; or*
(4) *Accept the risk.*

In a mature risk program, the results of risk assessments are evaluated with the entity's risk appetite into consideration. For example, if the entity has a Moderate Risk Appetite and there are several findings in a risk assessment that are High Risk, then action must be taken to reduce the risk. Accepting a High Risk would violate the Moderate Risk Appetite set by management. In reality, this leaves remediation, transferring or avoiding as the remaining three (3) options, since accepting the risk would be prohibited.

There are many ways to manage risk. However, the SCF's Security, Compliance & Resilience Cybersecurity & Data Privacy Risk Management Model (SCR-RMM) contains a control-centric:

- *Risk catalog;*
- *Threat catalog; and*
- *Methodology to not only perform a risk assessment, but manage risk across the entity.*

The value of the SCR-RMM is having a standardized methodology where controls are tied to specific risks and threats. Based on the other criteria offered by the SCF (e.g., weighting and maturity criteria), the SCR-RMM makes calculating risk a straightforward process.

Controls are the nexus of a cybersecurity and data protection program, so it is vitally important to understand how controls should be viewed from a high-level risk management perspective. To progress from identifying a necessary control to a determination of risk, it is a journey that has several steps, each with its own unique terminology. Therefore, it is important to baseline the understanding of risk management terminology.

6.10 SCRMS Principle 9: Evolve Processes

Cybersecurity and data protection measures must adapt and evolve to address business operations and the evolving threat landscape. This requires the adoption of a Plan, Do, Check & Act (PDCA) approach (e.g., Deming Cycle) to ensure the entity proactively identifies its requirements, implements appropriate protections, maintains situational awareness to detect incidents, operates a viable capability to respond to incidents and can sustain key business operations, if an incident occurs.

Things to consider when evolving processes:

- Changes in the compliance landscape (e.g., laws, regulations and contractual obligations);
- Technology changes; and
- Budget/resourcing constraints that affect how processes are implemented.

SCF Council Guidance

Things to consider when evolving processes:

- *Changes in the compliance landscape (e.g., laws, regulations and contractual obligations);*
- *Technology changes; and*
- *Budget/resourcing constraints that affect how processes are implemented.*

Without an overarching concept of operations for the SCRMS, entities will often find that their governance, risk management, compliance and data privacy teams are siloed in how they think and operate. These siloed functions and unclear roles often stem from a lack of a strategic understanding of how these specific functions come together to build a symbiotic working relationship between the individual teams that enables quality control over PPTDF.

The SCRMS utilizes a Plan, Do, Check & Act (PDCA) approach that is a logical way to design a governance structure:

(1) ***Plan***. *The overall SCRMS process beings with planning. This planning will define the policies, standards and controls for the entity. It will also directly influence the tools and services that an entity purchases, since technology purchases should address needs that are defined by policies and standards.*

(2) ***Do***. *Arguably, this is the most important section for cybersecurity and data protection practitioners. Controls are the "security glue" that make processes, applications, systems and services secure. Procedures (also referred to as control activities) are the processes in which the controls are actually implemented and performed.*

(3) ***Check***. *In simple terms, this is situational awareness. Situational awareness is only achieved through reporting through metrics and reviewing the results of audits/assessments.*

(4) ***Act***. *This is essentially risk management, which is an encompassing area that deals with addressing two main concepts (1) real deficiencies that currently exist and (2) possible threats to the entity.*

7 CONTROL SET DETERMINATION

The core of the SCRMS is the entity's control set. Controls are central to cybersecurity and data protection operations, as well as the overall business rhythm of any entity:

- Policies and standards should be hierarchically designed to support control objectives;
- Procedures are a form of control activity, describing how the control is operationalized; and
- Controls should be tied to metrics, threats and risks.

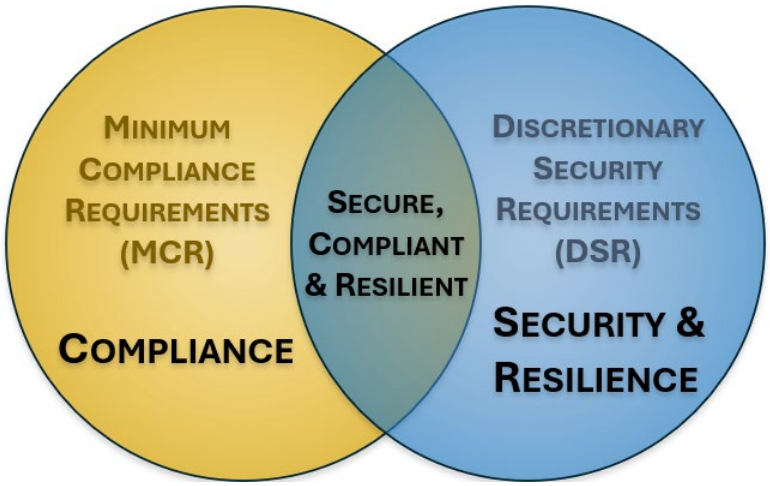
7.1 ESTABLISHING MINIMUM SECURITY REQUIREMENTS (MSR)

The combination of MCR and DSR equate to an entity's Minimum Security Requirements (MSR), which define the "must have" and "nice to have" requirements for PPTDF in one control set. It defines the Minimum Viable Product (MVP) technical and business requirements from a cybersecurity and data protection controls perspective.

Controls that comprise the MSR are expected to be applied to Technology Assets, Applications, Services and/or Data (TAASD) across the entity. ITGC provide the foundation of assurance for an entity's decision makers. MSR:

- Includes traditional IT General Controls (ITGC) controls; and
- Enables an entity's governance function to define how Technology Assets, Applications and Services (TAAS) are designed, implemented and operated.

Together, MCR and DSR form the entity's MSR.



7.2 LIVING CONTROL SET (LCS)

The concept of a Living Control Set (LCS) is to define the authoritative definition of what "reasonable security, compliance and resilience" means for the entity at a specific point in time. The LCS is not a static catalog of controls, nor is it a generic framework mapping. It is the entity-specific instantiation of control expectations derived from:

- MCR;
- DSR;
- The entity's risk appetite, risk tolerance and risk thresholds; and
- Explicit materiality criteria for risks, threats, incidents and controls.

The MSR defines the minimum defensible baseline required for the entity to demonstrate that its steady-state operations are secure, compliant and resilient:

- The MCR establishes the "ground floor" for compliance efforts that is based on non-negotiable obligations imposed by laws, regulations and contracts.
- The DSR represents risk-justified enhancements necessary to operate within the entity's defined risk tolerance and threat environment.
    - It is important to clarify that DSR are not optional enhancements, since the entity's risk, threat exposure, or materiality thresholds justify them; and

- DSR should be viewed as mandatory elements of the LCS, just as MCR are.

The LCS functions as the foundational layer of the SCRMS (e.g., SCRMS Principle #2). It establishes:

- What controls must exist;
- How those controls are prioritized;
- Which controls are considered material; and
- How control effectiveness is validated over time.

All subsequent governance, risk management, assessment and oversight activities operate against the LCS as the single source of truth.

7.2.1 Authoritative Nature of the LCS

The LCS is approved under the entity's defined governance authority (e.g., steering committee, CISO or GRC Director). Changes to the LCS must be documented, justified and traceable to one or more of the following:

- Changes in statutory, regulatory and/or contractual obligations;
- Emerging threats or shifts in risk exposure;
- Adjustments to risk appetite, tolerance and/or threshold;
- Lessons learned from incidents and/or capability testing; or
- Significant business changes (e.g., new products, acquisitions, divestitures, geographic expansion, etc.).

Managing the triggers for adjusting the LCS ensures that the definition of "reasonable" evolves deliberately, rather than informally.

7.2.2 Control Weighting and Material Controls

Not all controls are equal. Within the LCS, controls are assigned relative weighting to reflect their impact on the entity's ability to operate within its defined risk thresholds. Controls designated as material controls represent conditions where:

- No reasonable compensating control can offset their failure; and
- A deficiency would likely exceed defined materiality thresholds.

Material controls receive:

- Elevated maturity expectations;
- Increased oversight and reporting visibility;
- Priority in funding and remediation sequencing; and
- Explicit validation cadence requirements.

This weighting model prevents the false equivalence of controls commonly found in certification-driven management systems.

7.2.3 Evolution of the LCS

The LCS is referred to as "living" because it is subject to continuous governance review and modification. Its evolution is driven by:

- Evolving risk and threat landscape;
- Evolving compliance obligations;
- Results from conformity testing (e.g., control testing);
- Results from periodic risk assessments;
- Threat intelligence updates;
- Incident root cause analysis;
- Third-party risk findings; and
- Directives from the entity's strategic business planning cycles.

Updates to the LCS must preserve traceability so that historical decisions can be reconstructed for the possible scenarios where those decisions will be scrutinized by regulators, auditors, insurers and/or courts.

7.2.4 Governance and Oversight

The entity's mid-level and senior management roles are responsible for implementing and operating controls defined in the LCS.

The entity's executive leadership and the Board of Directors (BoD) are responsible for:

- Approving risk appetite and materiality thresholds;
- Reviewing material control status;
- Monitoring unresolved material risks; and
- Challenging assumptions regarding control effectiveness and risk exposure.

Through this separation, the LCS becomes the anchor for both due diligence (building capabilities) and due care (governing and evolving them).

7.2.5 Outcome

By defining, weighting and governing the LCS in this manner, the entity can demonstrate that:

- Controls were selected intentionally;
- Resources were allocated based on material risk;
- Oversight occurred at appropriate levels; and
- Security, compliance and resilience decisions were reasonable, documented and defensible.

The LCS is therefore not merely a control inventory, but the structural mechanism by which the SCRMS converts:

- Risk appetite into operational reality; and
- Operational activity into defensible evidence.

7.3 Minimum Compliance Requirements (MCR)

Compliance-related controls are viewed as "must have" requirements that are non-discretionary (e.g., not optional). These requirements are directly sourced from an entity's applicable laws, regulations and other obligations (e.g., contracts).

The process of clearly identifying non-discretionary controls generally involves interviewing multiple stakeholders to gain appropriate situational awareness of all pertinent compliance obligations. Stakeholders who can provide valuable insights are:

- Process owners;
- Procurement / Contracts Management;
- Project Management Office (PMO);
- Data Privacy;
- Enterprise Risk Management (ERM);
- Legal;
- Physical Security; and
- Human Resources.

7.3.1 Statutory Obligations

Statutory obligations are required by law and refer to current laws that were passed by a state or federal government. From a cybersecurity and data protection perspective, statutory compliance requirements include state, Federal and international laws. From a cybersecurity and data protection perspective, statutory compliance examples include, but are not limited to:

- Fair and Accurate Credit Transactions Act (FACTA);
- Family Education Rights and Privacy Act (FERPA);
- Federal Information Security Management Act (FISMA);
- Federal Trade Commission (FTC) Act;
- Gramm-Leach-Bliley Act (GLBA);
- Health Insurance Portability and Accountability Act (HIPAA);
- Sarbanes-Oxley Act (SOX);
- California - SB 1386 / CCPA / CPRA;
- Massachusetts - 201 CMR 17.00;
- Oregon - ORS 646A.622;
- Canada - Personal Information Protection and Electronic Documents Act (PIPEDA); and
- UK - Data Protection Act (DPA).

7.3.2 Regulatory Obligations

Regulatory obligations are required by law, but are different from statutory requirements in that these requirements refer to rules issued by a regulating body that is appointed by a state or federal government. These are legal requirements through proxy, where the regulating body is the source of the requirement. It is important to keep in mind that regulatory requirements tend to change more often than statutory requirements. From a cybersecurity and data protection perspective, regulatory compliance examples include, but are not limited to:

- Defense Federal Acquisition Regulation Supplement (DFARS);
- Federal Acquisition Regulation (FAR);
- Federal Risk and Authorization Management Program (FedRAMP);
- National Industrial Security Program Operating Manual (NISPOM);
- Financial Industry Regulatory Authority (FINRA);
- New York Department of Financial Services (NY DFS) 23 NYCRR 500; and
- European Union General Data Protection Regulation (EU GDPR).

7.3.3 Contractual Obligations

Contractual obligations are required by legal contract between private parties. This may be as simple as a cybersecurity or data privacy addendum in a vendor contract that calls out unique requirements. It also includes broader requirements from an industry association that membership brings certain obligations. From a cybersecurity and privacy perspective, common contractual compliance requirements include, but are not limited to:

- Payment Card Industry Data Security Standard (PCI DSS);
- ISO 27001 certification;
- Service Entity Control (SOC) audits; and
- Contractual requirement to adhere to a specific set of requirements, such as:
  - NIST Cybersecurity Framework;
  - Center for Internet Security Critical Security Controls (CIS CSC); and
  - Cloud Security Alliance Cloud Controls Matrix (CSA CCM).

7.4 Discretionary Security Requirements (DSR)

Cybersecurity and data protection controls that are not required by a law, regulation or contractual obligation are "nice to have" controls that are discretionary for an entity to implement. Any aspect of non-compliance with a discretionary control would be isolated within the realm of the stakeholder making the requirement, since the requirement is internal to the entity. The source of these discretionary requirements may be from:

- Board of Director (BoD) guidance;
- Steering Committee recommendations;
- Internal Audit findings;
- Prior incidents and/or events;
- Third-party audit/assessment recommendations; and/or
- Internal staff preferences.

The importance of these discretionary controls is that those are often entity-specific considerations to mitigate risk that is specific to an entity's business practices.

7.4.1 Discretionary Cybersecurity & Data Protection Considerations

A common frustration amongst cybersecurity practitioners is about the gaps that exist in many "best practice" cybersecurity frameworks that are used by entities to demonstrate a level of assurance (e.g., ISO 27001 certification, SOC 2 audit, CMMC certification, etc.). The remedy to address perceived gaps is through discretionary cybersecurity and data protection controls that are not directly mandated by a compliance obligation. Examples of discretionary controls, include but are not limited to:

- Data Loss Prevention (DLP);
- Network Access Control (NAC);
- File Integrity Monitoring (FIM);
- 24/7 Security Operations Center (SOC);
- Artificial Intelligence (AI) governance controls;
- Sandboxing / detonation chambers;
- Segmented development / test / production environments;
- Cloud infrastructure-specific controls; and

- Embedded technology-specific controls.

7.4.2 DISCRETIONARY RESILIENCE CONSIDERATIONS

NIST defines resilience as, *"The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."*[22] From a discretionary control perspective, this may require the addition of technologies and processes to help ensure the continuity of business operations, such as:

- Continuity of Operations Plan (COOP);
- Business Continuity / Disaster Recovery (BC/DR) Plan;
- Failover / redundancy capabilities;
- Business continuity test exercises;
- Offsite, online backup storage;
- Offsite, offline backup storage; and
- Transactional-level backups.

[22] *NIST Glossary - https://csrc.nist.gov/glossary/term/resilience#*

8 Due Diligence vs Due Care As Foundational Constructs of the SCRMS

The SCRMS defines what it means to be secure, compliant and resilient in a holistic, framework-agnostic manner to provide a structure that can help an entity demonstrate both:

- Due diligence in building secure, compliant and resilient capabilities; and
- Due care in governing and evolving them over time.

By explicitly integrating due diligence and due care, the SCRMS enables an entity to demonstrate that:

- Risks were identified and addressed in a structured manner;
- Capabilities were implemented based on known requirements, risks and threats;
- Deficiencies were tracked and managed based on risk-based prioritization;
- Oversight occurred at appropriate governance levels; and
- Decisions were documented and revisited as conditions evolved.

This approach aligns with expectations commonly applied when evaluating the reasonableness of security, compliance and resilience practices.

8.1 Due Diligence Considerations

Due diligence answers the question: *"Has the entity taken reasonable steps to build and operate secure, compliant and resilient capabilities?"*

NOTE: Due diligence refers to the reasonable design, implementation and operation of security, compliance and resilience capabilities based on known requirements, risks and business context.

Due diligence is about building capability in a way that is economically justified and risk-aligned, not just technically complete. Within the SCRMS, due diligence includes:

- Establishing governance structures and authority;
- Defining the entity's cybersecurity and data protection controls, based on:
  - Applicable statutory, regulatory and contractual obligations; and
  - Risk-based requirements and industry expectations that augment compliance obligations;
- Implementing security, compliance and resilience capabilities in a structured, prioritized manner; and
- Producing objective evidence that controls exist and operate as intended.

8.2 Due Care Considerations

Due care answers the question: *"Is leadership actively governing and adapting SCR capabilities in response to changing risks and conditions?"*

NOTE: Due care refers to the ongoing oversight, validation and evolution of security, compliance and resilience capabilities after those capabilities are implemented and operational.

Due care is what protects directors and officers by demonstrating informed oversight and documented risk decisions. Within the SCRMS, due care includes:

- Executive-level oversight and accountability;
- Situational awareness of risk and threat exposure;
- Validation of control effectiveness;
- Risk acceptance and prioritization tied into Enterprise Risk Management (ERM); and
- A commitment to improve capabilities as conditions change.

9 INTEGRATING SECURITY, COMPLIANCE & RESILIENCE INTO BUSINESS PLANNING ACTIVITIES

The Security, Compliance & Resilience Management System (SCRMS) is designed to integrate with an entity's broader business planning activities, so that by design the capabilities exist to be secure, compliant and resilient, while meeting the business and technical requirements. This "security, compliance and resilience ecosystem" mindset is meant to exist beyond just typical cybersecurity and data protection functions.

9.1 TRUSTED ADVISOR GUARDRAIL

The cybersecurity industry is renowned for marketing professional services as a "trusted advisor" to an entity's executive leadership. Essentially, this is the process of telling an entity's leaders what steps to take next, as part of a broader journey that never ends.

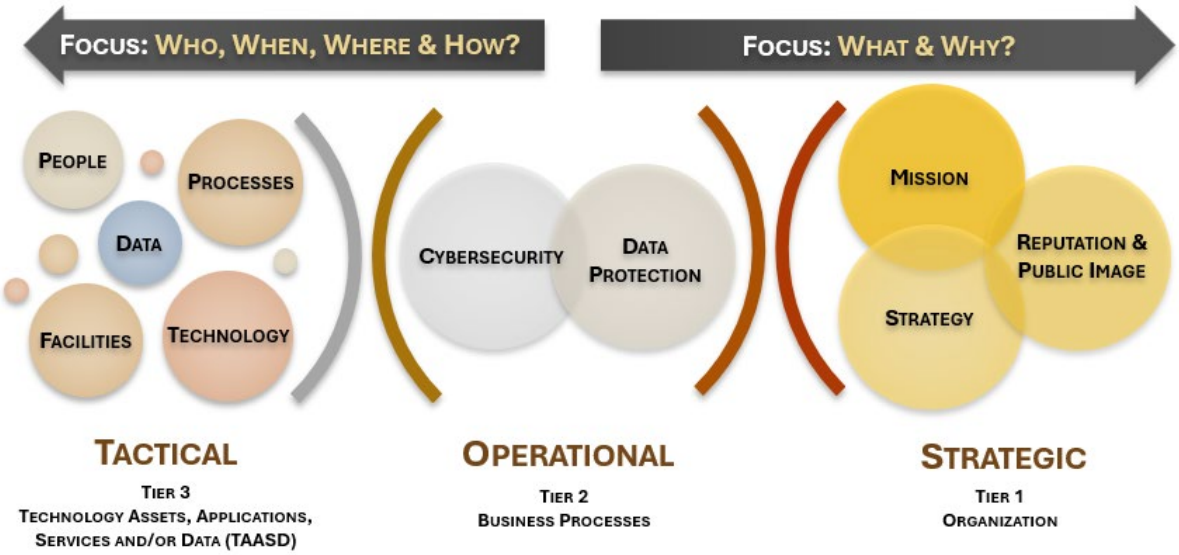
The SCRMS provides a means to minimize Fear, Uncertainty and Doubt (FUD) by focusing on capabilities that reasonably need to exist to be secure, compliant and resilient. This is where the SCRMS can act as a "guardrail" to ensure advice from internal and third-parties enables secure, compliant and resilient practices.

Minimizing FUD can be achieved by focusing on these questions:

(1) Is this approach defensible?
(2) Does this approach reduce reinterpretation?
(3) Does this approach preserve meaning over time?
(4) Does this approach make maturity easier to explain?
(5) Does this approach help scale without additional headcount?

9.2 PRIORITIZED ROADMAP CONCEPT

Practically, the SCRMS should be leveraged to create a prioritized roadmap that is based on a hierarchical, risk-based approach to successfully accomplishing the entity's stated goals. From a top-down perspective, the SCRMS can assist decision makers understand the variables the make-up the *"Who? What? When? Where? How? and Why?"* questions that arise in the process of designing, implementing and maintaining secure, compliant and resilient capabilities.



9.2.1 TIER 1 – STRATEGIC OBJECTIVES

Tier 1 provides strategic management direction using entity-level mission/business goals, policies, governance structures and entity-wide resource allocation. Tier 1 activities help to ensure that cybersecurity and data protection strategies are cost-effective, efficient and consistent with the broader strategic goals and objectives of the entity.

9.2.2 Tier 2 – Operational Objectives

Tier 2 addresses security, compliance and resiliency from a mission/business process perspective and is informed by the context established at Tier 1. In this tier, program requirements are defined and managed, including cost, schedule, performance and a variety of critical nonfunctional requirements. These nonfunctional requirements include concepts such as reliability, dependability, safety, security and quality. Many threats to and through the supply chain are addressed at this level in the management of trust relationships with system integrators, suppliers and external service providers of technology-related products and services.

9.2.3 Tier 3 – Tactical Objectives

Tier 3 is where security, compliance and resiliency activities are integrated into the entity's Technology Assets, Applications, Services and/or Data (TAASD), prioritized by the context established at Tier 2.

9.3 SCRMS Governance Considerations – Potential Gaps & Exposures

Entities are expected to tailor the implementation of the SCRMS for their specific needs, based on applicable People, Processes, Technology, Data and/or Facilities (PPTDF).

The following topics address areas of potential gaps that entities must avoid assumptions on. This requires due diligence and due care actions to avoid, or minimize, potential gaps and/or exposures.

9.3.1 Operational Control Assumptions

A potential capabilities gap exists for operational control assumptions. This issue is based on how SCRMS assumes governance intent translates into execution without explicitly enforcing operational control mechanisms.

Problematic issues associated with potential capabilities gap include, but are not limited to:

(1) Compliance without operational stability; and
(2) Periods of time where security and resilience capabilities diminish between audits.

9.3.2 Due Care Verifiability

A potential capabilities gap exists for due care verifiability. This issue is based on due care activities that are conceptually defined but lack defensible, evidence-based proof requirements.

Problematic issues associated with potential capabilities gap include, but are not limited to:

(1) "Security theater" where due care activities are merely theoretical through documentation; and
(2) Available defensible evidence is insufficient to demonstrate reasonable due care practices.

9.3.3 Control Drift & Capability Decay

A potential capabilities gap exists for control drift and capability decay. This issue is based on scenarios when there are no explicit mechanisms to detect or prevent control erosion caused by routine change.

Problematic issues associated with potential capabilities gap include, but are not limited to:

(1) Point-in-time snapshot compliance instead of durable security posture; and
(2) Governance practices lose focus on security, compliance and resilience prioritization.

9.3.4 AI Governance Depth

A potential capabilities gap exists for the depth of AI governance. This issue is based on AI being treated as a risk category, not as a governed lifecycle system.

Problematic issues associated with potential capabilities gap include, but are not limited to:

(1) AI governance is run as a siloed activity that negatively affects situational awareness across the entity; and
(2) Cross-functional expertise does not exist to properly perform AI governance activities.

9.3.5 Supply Chain Threats

A potential capabilities gap exists for Third-Party Risk Management (TPRM) governance. This issue is based on TPRM treated as an extension, not a co-equal attack surface.

Problematic issues associated with potential capabilities gap include, but are not limited to:

(1) "Check box" approach to security, compliance and resilience reviews for third-parties, where pertinent risks and threats are ignored for misguided efficiency purposes; and
(2) Indirect compromise despite evidence of conformity.

9.3.6 Decision Making Authority

A potential capabilities gap exists for authority to make decisions. This issue is based on roles being defined, but decision authority and escalation paths are unclear.

Problematic issues associated with potential capabilities gap include, but are not limited to:

(1) A lack of designated alternative decision-makers; and
(2) Governance paralysis during incidents.

9.3.7 Resilience Stress Testing

A potential capabilities gap exists for resilience stress testing. This issue is based on scenarios where resilience planning lacks compounded, adversarial stress testing requirements.

Problematic issues associated with potential capabilities gap include, but are not limited to:

(1) Misunderstanding of service dependencies provides gaps in resilience planning activities; and
(2) False confidence in resilience capabilities.

9.3.8 Linear Maturity Assumptions

A potential capabilities gap exists for maturity assumptions. This issue is based on maturity models that assume rational progression.

Problematic issues associated with potential capabilities gaps include, but are not limited to:

(1) Incorrect assumption that all controls are weighted equally for maturity planning needs (e.g., material controls); and
(2) Misleading maturity scores.

9.3.9 Metrics Without Guardrails

A potential capabilities gap exists for metrics and analytics governance. This issue is based on scenarios where Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) are encouraged without defining metrics that may be misleading and lead to false assumptions.

Problematic issues associated with potential capabilities gap include, but are not limited to:

(1) Developing metrics that are not "SMART":
    a. Specific;
    b. Measurable;
    c. Achievable;
    d. Relevant; and
    e. Time-bound; and
(2) Executive dashboards may mask systemic risk.

9.3.10 Economic Decision Framing

A potential capabilities gap exists for framing decisions that ignore economic realities for the entity. This issue is based on the absence of an explicit economic model for security tradeoffs.

Problematic issues associated with potential capabilities gap include, but are not limited to:

(1) Potential instances of negligent behaviors, based on low maturity capabilities; and
(2) Underfunded or strategically rejected programs.

9.4 Surviving Real-World Challenges

From a governance perspective, the following questions should be addressed to determine if an entity's SCRMS is capable of surviving real-world challenges:

Challenge Area	Real-World Capability Question
Operational Reality	*"What prevents security, compliance and resilience controls from being undermined by routine operational change?"*
Evidence Integrity	*"How does SCRMS distinguish real operational execution from performative documentation?"*
Control Longevity	*"How does SCRMS detect and correct control decay between formal assessments?"*
AI Accountability	*"Who owns AI decisions, failures and unintended consequences under SCRMS?"*
Vendor Breach Scenarios	*"How does SCRMS respond when a trusted third party becomes the breach vector?"*
Decision Authority	*"Who has final authority during security and resilience conflicts or crises?"*
Resilience Proof	*"Has resilience been proven under compounded failure scenarios?"*
Maturity Honesty	*"How does SCRMS prevent maturity scoring from becoming aspirational fiction?"*
Metric Validity	*"Which metrics are explicitly disallowed due to false confidence risk?"*
Business Alignment	*"How does SCRMS support rational economic decisions rather than idealized security goals?"*

10 NESTED APPROACH TO RISK MANAGEMENT PRACTICES

The alternative to risk management is crisis management. Risk management is a multi-layered capability. From a cybersecurity and data protection perspective, there should be at least three (3) layers of risk management focus:

(1) Enterprise Risk Management (ERM);
(2) Cybersecurity & Data Protection Risk Management (CDPRM); and
(3) Third-Party Risk Management (TPRM) (inclusive of Supply Chain Risk Management (SCRM) activities).

Similar in concept to traditional "Russian nesting dolls," from a risk management hierarchy perspective:

- TPRM should be subordinate to CDPRM; and
- CDPRM should be subordinate to ERM.

10.1 RISK PROFILE

Per NIST, a risk profile is a *"prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks."* [23] The ability to prioritize and assess risks requires the entity to create entity-specific definitions and associated criteria for:

(1) Risk appetite;
(2) Risk tolerance; and
(3) Risk threshold.

The reasoning for this is simple – the entity needs to speak the same language for risk management operations, where everyone understands the thresholds associated with low, moderate, high, etc. risks. Only through this level of standardization will an entity be able to efficiently and effectively manage risk associated with Technology Assets, Applications, Services and/or Data (TAASD).

10.1.1 RISK APPETITE

A risk appetite is a broad "risk management concept" used to inform employees about what is and is not acceptable, regarding risk management from an entity's executive leadership team. A risk appetite does not contain granular risk management criteria and is primarily a "management statement" that is subjective. Similar in concept to how a policy is a *"high-level statement of management intent,"* an entity's defined risk appetite is a high-level statement of how all risk, or certain types of risk, are willing to be accepted.

10.1.2 RISK TOLERANCE

Risk tolerance is based on objective criteria, unlike the subjective, conceptual nature of a risk appetite. Defining objective criteria is a necessary step to categorize risk on a graduated scale. Establishing objective criteria to quantify the impact of risk enables risk assessments to leverage those same criteria and assist decision-makers in their risk management decisions (e.g., accept, mitigate, transfer or avoid).

10.1.3 RISK THRESHOLDS

Risk thresholds are directly tied to risk tolerance and utilize entity-specific criteria (e.g., acceptable and unacceptable parameters). These risk thresholds exist between the different levels of risk tolerance (e.g., Low, Moderate and High Risk). By establishing these risk thresholds, it provides a means of comparing relative risk to an entity. Risk thresholds are criteria that are unique to an entity such as entity-specific activities / scenarios that could:

- Damage the entity's reputation;
- Negatively affect short-term and long-term profitability; and/or
- Impede business operations.

[23] *NIST Glossary for Risk Profile - https://csrc.nist.gov/glossary/term/risk_profile*

Risk thresholds are entirely unique to each entity, based on several factors that include:

- Financial stability;
- Management preferences;
- Compliance obligations (e.g., statutory, regulatory and/or contractual); and
- Insurance coverage limits.

10.2 MATERIALITY

Defining materiality is an executive leadership determination, not a cybersecurity determination. This is entity-specific and is primarily based on a clearly-defined financial threshold.

Once the materiality threshold is clearly defined, it then requires a look at an entity's risk and threat management practices to identify those specific risks and threats that could lead to a material incident. Ideally, this means reviewing established risk and threat catalogs to identify known risks and threats that have material implications.

The SCF Council defines the materiality threshold for an entity's cybersecurity and data protection program as, *"A deficiency, or a combination of deficiencies, in an entity's cybersecurity and/or data protection controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the entity can adhere to its stated risk tolerance."* [24]

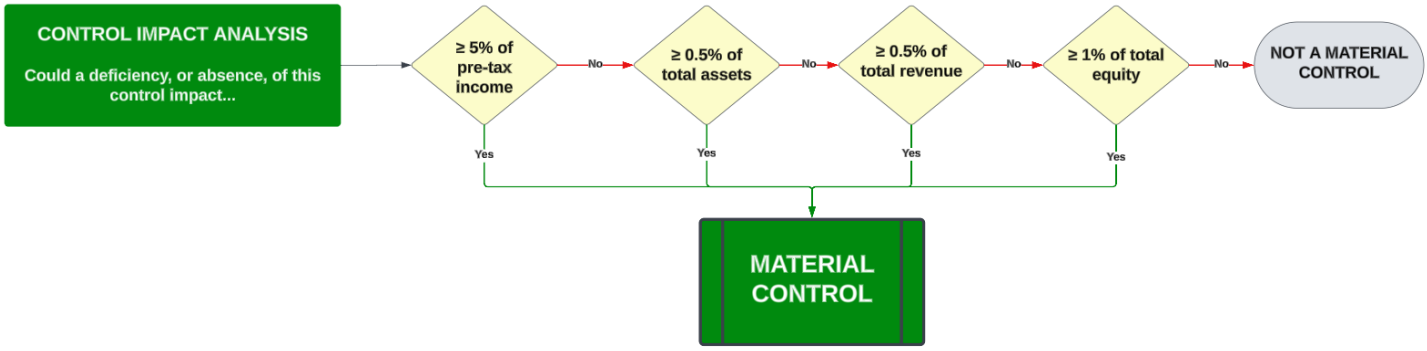
Generally, account criteria from pre-tax income, total assets, total revenue and total equity to provide options for both "single criteria determinations" and "averaged determinations" to establish objective thresholds. From a financial benchmark perspective, for something to be considered material, the control deficiency, risk, threat or incident (singular or a combination) generally must meet one, or more, of the following criteria where the potential financial impact is measured as:[25]

- ≥ 5% of Earnings Before Tax (EBT) (e.g., total revenue after subtracting expenses, except taxes);
- ≥ 0.5% of total assets (e.g., net book value of tangible and intangible assets);
- ≥ 1% of total equity (e.g., residual value of the entity after subtracting liabilities); and/or
- ≥ 0.5% of total revenue (e.g., gross sales plus other income).

10.2.1 MATERIAL CONTROL IDENTIFICATION

When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. A material control is such a fundamental cybersecurity and/or data protection control that:

- It is not capable of having compensating controls; and
- Its absence, or failure, exposes an entity to such a degree that it could have a material impact.

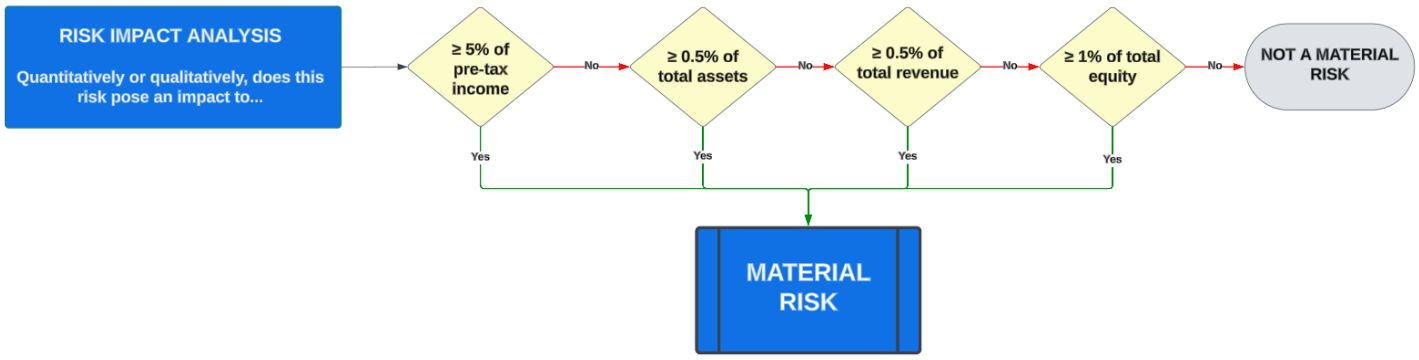


10.2.2 MATERIAL RISK IDENTIFICATION

When an identified risk that poses a material impact, that is a material risk. A material risk:

- Is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.); and
- Should be identified and documented in an entity's "risk catalog" that chronicles the entity's relevant and plausible risks.

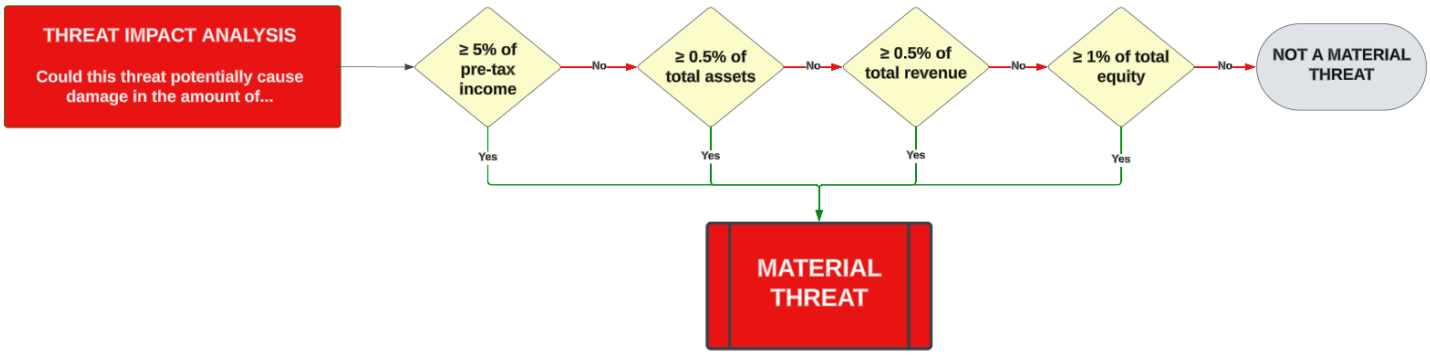
[24] *SCF Cybersecurity Materiality - https://securecontrolsframework.com/cybersecurity-materiality/*
[25] *Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf*



10.2.3 Material Threat Identification

When an identified threat poses a material impact, that is a material threat. A material threat:

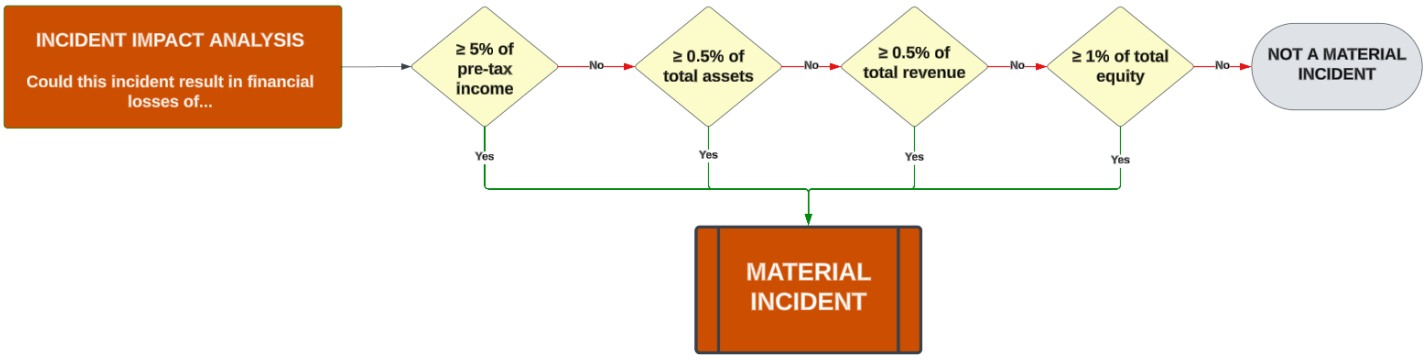
- Is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and
- Should be identified and documented in an entity's "threat catalog" that chronicles the entity's relevant and plausible threats.



10.2.4 Material Incident Identification

When an incident poses a material impact, that is a material incident. A material incident is an occurrence that does or has the potential to:

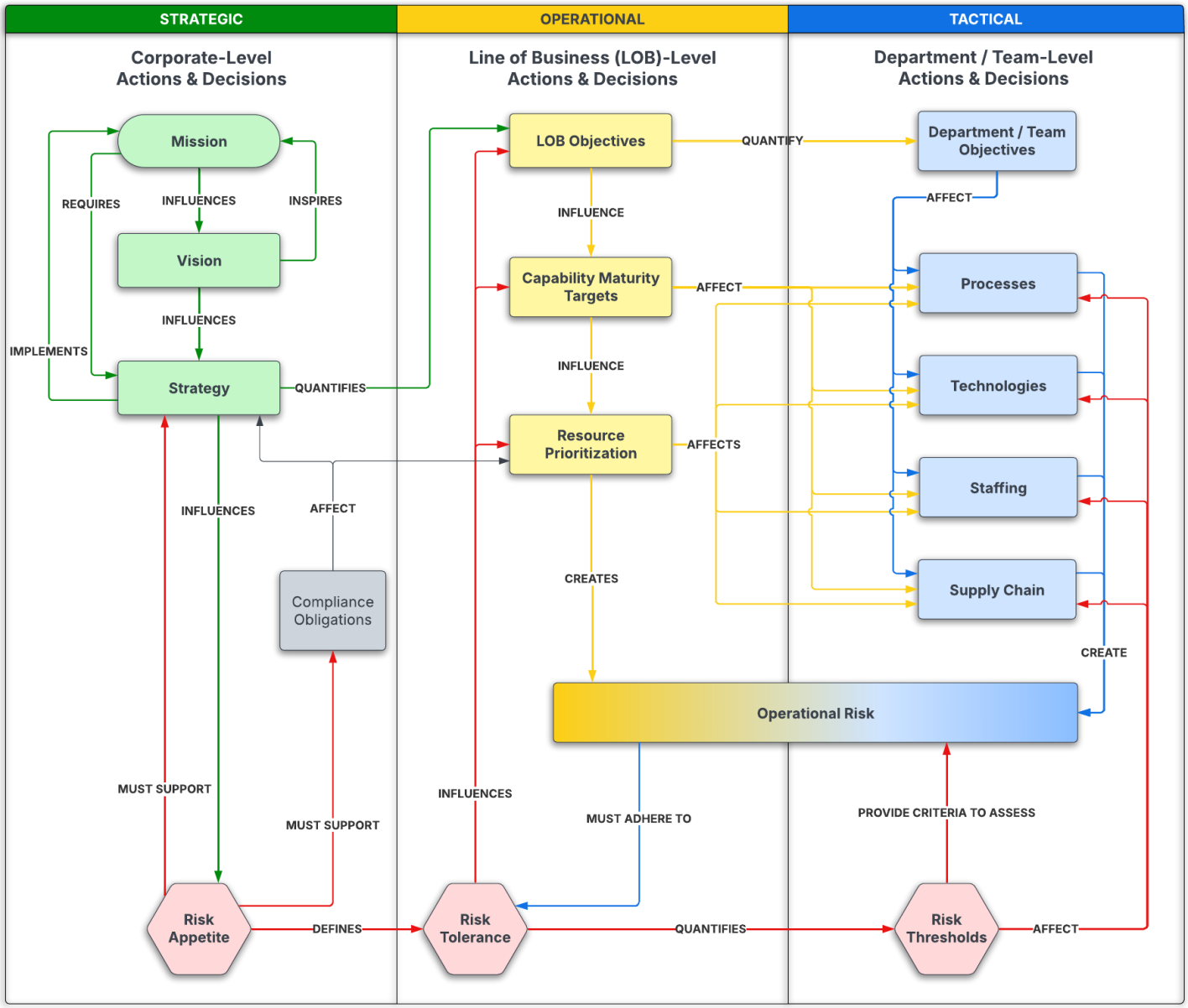
- Jeopardize the Confidentiality, Integrity, Availability and/or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits with a material impact on the entity; and/or
- Constitute a violation, or imminent threat of violation, of an entity's policies, standards, procedures or acceptable use practices that has a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.).



10.3 Integration of Risk Management & Business Planning

These key concepts of how risk appetite, risk tolerance and risk thresholds interact with strategic, operational and tactical actions and decisions can be visualized in the following graphic:

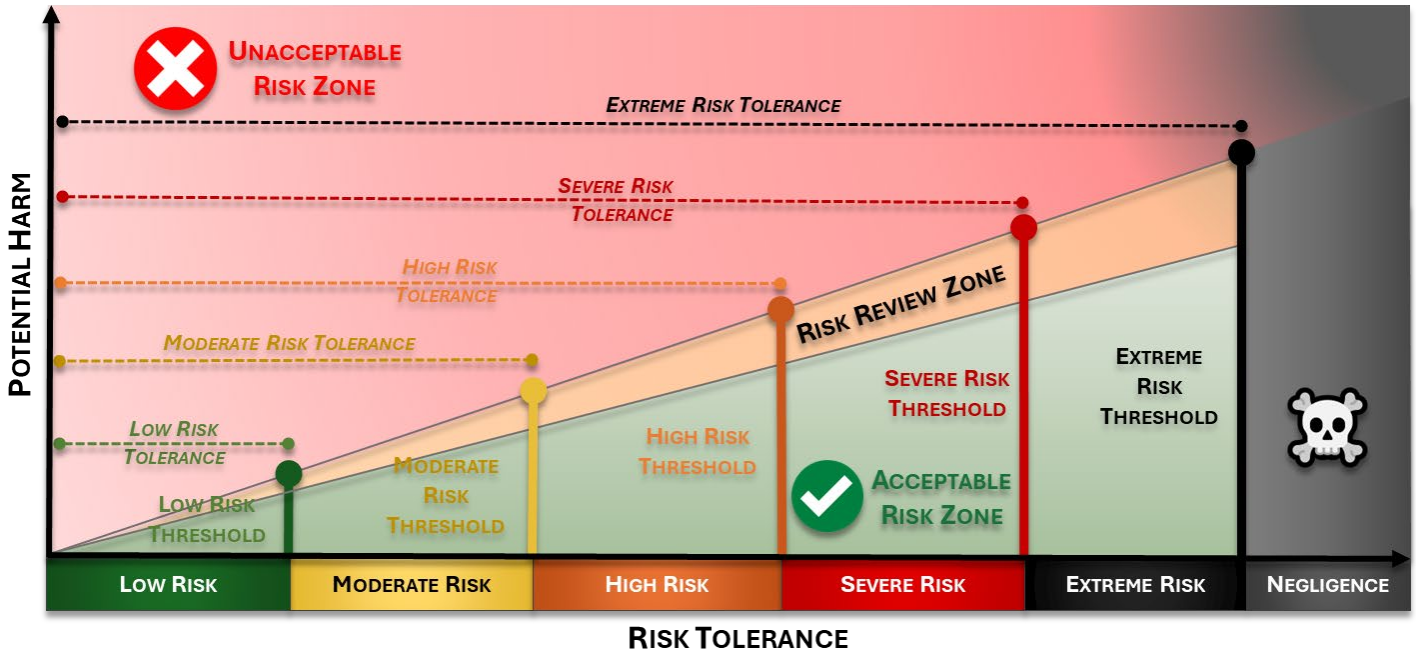
- At the strategic layer, where corporate-level actions and decisions are made, the entity's risk appetite is defined. The scope of the risk appetite can be entity-wide or compartmentalized to provide enhanced granularity.
- At the operational level, where Line of Business (LOB)-level actions and decisions are made, the entity's risk tolerance is put into practice. The entity's risk tolerance is defined by its established risk appetite.
- At the tactical level, where department / team-level actions and decisions are made, the entity's risk thresholds are used to provide criteria to assess operational risk. That operational risk must adhere to the entity's risk tolerance and therefore, its risk appetite.



10.4 Enterprise Risk Management (ERM)

ERM focuses on risk management at the entity level. ERM is expected to clearly define the criteria that constitute what is allowed and what is prohibited from a risk management perspective:

(1) Acceptable Risk. The criteria fall within a range of acceptable parameters; and
(2) Unacceptable Risk. The criteria fall outside a range of acceptable parameters.



10.5 Cybersecurity & Data Protection Risk Management (CDPRM)

CDPRM focuses on the cybersecurity and data protection component of risk management. CDPRM is expected to operate within the parameters established by ERM to ensure entity-wide risk management guidance is implemented.

10.6 Third-Party Risk Management (TPRM)

TPRM focuses on external risks associated with third-parties. This includes, but is not limited to:

- External Service Providers (ESP);
- Cloud Service Providers (CSP); and
- Material suppliers.

Sub-component of TPRM involve:

- Supply Chain Risk Management (SCRM);
- Cybersecurity Supply Chain Risk Management (C-SCRM).

Within the scope of the SCRMS, supply chain-related risks and threats are inclusive of third-party governance practices.

11 DUE DILIGENCE ACTIVITIES

As described in Section 7 – Control Set Determination, the Minimum Security Requirements (MSR) is a baseline determined by the entity's Minimum Compliance Requirements (MCR) and Discretionary Security Requirements (DSR). While compliance-related activities are unique to the statutory, regulatory or contractual obligations of the entity, there are reasonable cybersecurity and data protection capabilities that entities should implement, regardless of its size, industry or geography. These foundational practices are part of the SCF's Cybersecurity Oversight, Resilience and Enablement (SCF CORE) Fundamentals baseline, designed to:[26]

(1) Contain administrative, technical and physical safeguards for the protection of Technology Assets, Applications, Services and/or Data (TAASD); and
(2) Protect against any reasonable risks and threats.

From a due diligence perspective for the SCRMS, an entity is expected to demonstrate conformity with the following practices:

11.1 CYBERSECURITY & DATA PROTECTION GOVERNANCE

The entity must specify the development of its cybersecurity and data protection program, including criteria to measure success, to ensure ongoing leadership engagement and risk management.

Relevant SCF Control(s):
- GOV-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An entity-wide cybersecurity and data protection governance program is developed.
(2) The cybersecurity and data protection governance program addresses management commitment.
(3) The cybersecurity and data protection governance program addresses statutory, regulatory and/or contractual compliance obligations.

11.1.1 STEERING COMMITTEE & PROGRAM OVERSIGHT

The entity must coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.

Relevant SCF Control(s):
- GOV-01.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An executive steering committee, or advisory board, is formed and is comprised of key cybersecurity, technology, risk, privacy and business executives.
(2) The executive steering committee, or advisory board, coordinates cybersecurity, technology, risk, privacy and business alignment through recurring, formal meetings.

11.1.2 PUBLISHING CYBERSECURITY & DATA PROTECTION DOCUMENTATION

The entity must establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.

Relevant SCF Control(s):
- GOV-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Cybersecurity and data protection policies are developed and documented.

[26] *SCF CORE Fundamentals - https://securecontrolsframework.com/core/*

(2) *Policies needed to satisfy the security requirements for the protection of sensitive and/or regulated data are:*
    a. *Developed and documented; and*
    b. *Disseminated to the entity's personnel or roles.*
(3) *Procedures needed to satisfy the security requirements for the protection of sensitive and/or regulated data are:*
    a. *Developed and documented; and*
    b. *Disseminated to the entity's personnel or roles.*

11.1.3 Exception Management

The entity must prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.

Relevant SCF Control(s):
- GOV-02.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Exception requests to standards are formally submitted for review, along with a business justification for the deviation and proposed compensating controls.*
(2) *The exception request undergoes a risk assessment to evaluate the business justification and proposed compensating controls.*
(3) *A documented determination is made to approve or deny the exception request.*
(4) *The requestor of the exception is provided a response on the determination including required actions, if applicable.*

11.1.4 Assigned Cybersecurity & Data Protection Responsibilities

The entity must assign a qualified individual with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity and data protection program.

Relevant SCF Control(s):
- GOV-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *A senior cybersecurity position is appointed.*
(2) *The senior cybersecurity position is provided with the mission and resources to coordinate, develop, implement and maintain an entity-wide cybersecurity and data protection program.*

11.1.5 Stakeholder Accountability Structure

The entity must 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.

Relevant SCF Control(s):
- GOV-04.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *The cybersecurity and data protection governance program includes the identification and assignment of roles.*
(2) *The cybersecurity and data protection governance program includes the identification and assignment of responsibilities.*

11.1.6 Establish Context For Business Operations

The entity must define the context of its business model and document its mission.

Relevant SCF Control(s):
- GOV-08: Defining Business Context & Mission

NOTE: Establishing the context for business operations is a component of SCRMS Principle 1. Clarity in how the business operates, including a clearly-defined mission, provides context for security, compliance and resilience requirements.

(1) The entity's mission is clearly defined and documented.

(2) The entity's executive leadership defines and documents a formal business strategy that is used to provide operational guidance to key business leaders across the entity.

11.1.7 Operationalizing Cybersecurity & Data Protection Practices

The entity must compel data and/or process owners to operationalize cybersecurity and data protection practices for Technology Assets, Applications and/or Services (TAAS) under their control.

Relevant SCF Control(s):

- GOV-15

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Roles and responsibilities exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each system, application and/or service under their control.

(2) Individual Contributor (IC) performance reviews cover how data and/or process owners operationalized cybersecurity and data protection practices for each system, application and/or service under their control.

(3) Systems security engineering principles are applied to the development or modification of the system and system components.

11.1.8 Select Controls

The entity must compel data and/or process owners to select required cybersecurity and data protection controls for each TAAS under their control.

Relevant SCF Control(s):

- GOV-15.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Roles and responsibilities exist to compel data and/or process owners to select required cybersecurity / data privacy controls for each system, application and/or service under their control.

(2) Individual Contributor (IC) performance reviews cover how data and/or process owners select required cybersecurity / data privacy controls for each system, application and/or service under their control.

11.1.9 Implement Controls

The entity must compel data and/or process owners to implement required cybersecurity and data protection controls for each TAAS under their control.

Relevant SCF Control(s):

- GOV-15.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Roles and responsibilities exist to compel data and/or process owners to implement required cybersecurity / data privacy controls for each system, application and/or service under their control.

(2) Individual Contributor (IC) performance reviews cover how data and/or process owners implement required cybersecurity / data privacy controls for each system, application and/or service under their control.

11.1.10 Assess Controls

The entity must compel data and/or process owners to assess if required cybersecurity and data protection controls for each TAAS under their control are implemented correctly and are operating as intended.

Relevant SCF Control(s):

- GOV-15.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Roles and responsibilities exist to compel data and/or process owners to assess if required cybersecurity / data privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.

(2) Individual Contributor (IC) performance reviews cover how data and/or process owners assess if required cybersecurity / data privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.

11.1.11 Authorize Technology Assets, Applications and/or Services (TAAS)

The entity must compel data and/or process owners to obtain authorization for the production use of each TAAS under their control.

Relevant SCF Control(s):

- GOV-15.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) 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.

(2) 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.

11.1.12 Materiality Determinations

The entity must define materiality threshold criteria capable of designating an incident as material.

Relevant SCF Control(s):

- GOV-16

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Entity-specific criteria to define a materiality threshold capable of designating an incident as material is documented.

11.1.13 Material Risks

The entity must define criteria necessary to designate a risk as a material risk.

Relevant SCF Control(s):

- GOV-16.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Entity-specific criteria to designate a risk as a "material risk," as it pertains to materiality considerations, is documented.

11.1.14 Material Threats

The entity must define criteria necessary to designate a threat as a material threat.

Relevant SCF Control(s):

- GOV-16.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Entity-specific criteria to designate a threat as a "material threat," as it pertains to materiality considerations, is documented.*

11.2 Artificial Intelligence & Autonomous Technologies

The entity must ensure Artificial Intelligence (AI) and autonomous technologies are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced. In addition, AI-related risks are governed according to minimize emergent properties or unintended consequences.

Relevant SCF Control(s):

- AAT-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *AAT-specific policies, standards and procedures are:*
   a. *Developed and documented; and*
   b. *Implemented effectively.*
(2) *AAT operations are conducted according to documented policies, standards, procedures and/or other entity directives.*
(3) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support AAT operations.*
(4) *Responsibility and authority for the performance of AAT-related activities are assigned to designated personnel.*

11.2.1 Artificial Intelligence (AI) & Autonomous Technologies Governance

The entity must 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.

Relevant SCF Control(s):

- AAT-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *AAT-specific policies, standards and procedures are:*
   a. *Developed and documented; and*
   b. *Implemented effectively.*
(2) *AAT operations are conducted according to documented policies, standards, procedures and/or other entity directives.*
(3) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support AAT operations.*
(4) *Responsibility and authority for the performance of AAT-related activities are assigned to designated personnel.*

11.2.2 Trustworthy AI & Autonomous Technologies

The entity must ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced to minimize emergent properties or unintended consequences.

Relevant SCF Control(s):

- AAT-01.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Secure engineering principles are defined.*
(2) *Data privacy engineering principles are defined.*

11.2.3 Situational Awareness of AI & Autonomous Technologies

The entity must develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).

Relevant SCF Control(s):
- AAT-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An inventory of systems and system components that is at the level of granularity deemed necessary for tracking and reporting is documented.

11.2.4 Adequate Protections For AI & Autonomous Technologies

The entity must ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) include reasonable cybersecurity and data protections that are commensurate with assessed risks and threats.

Relevant SCF Control(s):
- AAT-02.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Risks and threats for AAT are identified.

(2) Reasonable cybersecurity and data protections that are commensurate with assessed risks and threats AAT are:

a. Defined; and

b. Implemented.

11.2.5 Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)

The entity must implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.

Relevant SCF Control(s):
- AAT-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The entity's Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) capability is entity-wide.

(2) A process is implemented to ensure that the entity's plans for conducting cybersecurity and data protection testing, training and monitoring activities associated with the entity's systems are:

a. Developed; and

b. Maintained.

(3) A process is implemented to ensure that the entity's plans for conducting cybersecurity and data protection testing, training and monitoring activities associated with the entity's systems continue to be executed.

(4) The authorization processes are integrated into an entity-wide risk management program.

11.3 Asset Management

The entity must 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 entity's network and to protect the entity's data that is stored, processed or transmitted on its assets.

Relevant SCF Control(s):
- AST-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *An authoritative source and repository are established to provide a trusted source and accountability for approved and implemented systems and system components.*
(2) *The frequency at which to review / update the system and system component inventory is defined.*
(3) *An inventory of systems and system components that is at the level of granularity deemed necessary for tracking and reporting is developed and documented.*
(4) *IT Asset Management (ITAM) operations are conducted according to documented policies, standards, procedures and/or other entity directives.*
(5) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support ITAM operations.*
(6) *Responsibility and authority for the performance of ITAM-related activities are assigned to designated personnel.*

11.3.1 Asset-Service Dependencies

The entity must identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.

Relevant SCF Control(s):
- AST-01.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Asset-service dependencies are:*
    a. *Identified;*
    b. *Documented; and*
    c. *Assessed to evaluate cybersecurity and data protection concerns for technology assets that support more than one critical business function.*

11.3.2 Stakeholder Identification & Involvement

The entity must identify and involve pertinent stakeholders of critical TAASD to support the ongoing secure management of those assets.

Relevant SCF Control(s):
- AST-01.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Pertinent stakeholders of critical systems, applications and services are:*
    a. *Identified and documented; and*
    b. *Involved in supporting the ongoing secure management of those assets.*

11.3.3 Asset Inventories

The entity must perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that:
(1) Accurately reflects the current TAASD in use;
(2) Identifies authorized software products, including business justification details;
(3) Is at the level of granularity deemed necessary for tracking and reporting;
(4) Includes entity-defined information deemed necessary to achieve effective property accountability; and
(5) Is available for review and audit by designated the entity's personnel.

Relevant SCF Control(s):
- AST-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *A documented, up-to-date, complete, accurate and readily available inventory of systems and system components exists.*
(2) *The system inventory includes hardware, software, firmware and documentation.*

(3) *The inventory is maintained (reviewed / updated) throughout the system development life cycle.*
(4) *Per an entity-defined frequency, the system component inventory is:*
    a. *Reviewed; and*
    b. *Updated.*

11.3.4 Data Action Mapping

The entity must create and maintain a map of Technology Assets, Applications and/or Services (TAAS) where sensitive and/or regulated data is stored, transmitted or processed.

Relevant SCF Control(s):
- AST-02.8

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *A map of system data actions is developed and documented.*
(2) *The location of sensitive and/or regulated data is identified and documented.*
(3) *The system components on which sensitive and/or regulated data is processed are identified and documented.*
(4) *The system components on which sensitive and/or regulated data is stored are identified and documented.*
(5) *Changes to the system or system component location where sensitive and/or regulated data is processed are documented.*
(6) *Changes to the system or system component location where sensitive and/or regulated data is stored are documented.*

11.3.5 Network Diagrams & Data Flow Diagrams (DFDs)

The entity must maintain network architecture diagrams that:
(1) Contain sufficient detail to assess the security of the network's architecture;
(2) Reflect the current architecture of the network environment; and
(3) Document all sensitive and/or regulated data flows.

Relevant SCF Control(s):
- AST-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Sensitive data flows are identified and documented.*
(2) *A Data Flow Diagram (DFD) exists for each type of sensitive and/or regulated data that is stored, processed and/or transmitted.*
(3) *A process exists to review DFDs for accuracy.*
(4) *A process exists to update DFDs upon technology or business practice changes that affect where sensitive and/or regulated data is stored, processed and/or transmitted.*
(5) *One or more high-level network diagrams exist as a schematic to identify the logical placement of systems, applications and services at a conceptual level.*
(6) *One or more low-level network diagrams exist as a schematic to identify the detailed logical and physical placement of systems, applications and services.*
(7) *A process exists to review network diagrams for accuracy.*
(8) *A process exists to update network diagrams upon technologies change.*

11.3.6 Secure Disposal, Destruction or Re-Use of Equipment

The entity must securely dispose of, destroy or repurpose system components using entity-defined techniques and methods to prevent information being recovered from these components.

Relevant SCF Control(s):
- AST-09

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Data, documentation, tools or system components to be disposed of are defined.*
(2) *Techniques and methods for disposing of data, documentation, tools or system components are defined.*
(3) *Data, documentation, tools or system components are disposed of using techniques and methods.*
(4) *System media is sanitized using sanitization techniques and procedures prior to disposal.*

11.3.7 Bring Your Own Device (BYOD) Usage

The entity must implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.

Relevant SCF Control(s):
- AST-16

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *A Bring Your Own Device (BYOD) program is implemented and governed to reduce risk associated with personally-owned devices in the workplace.*

11.4 Business Continuity & Disaster Recovery

The entity must establish processes that will help the entity recover from adverse situations with minimal impact to operations, as well as provide the capability for e-discovery.

Relevant SCF Control(s):
- BCD-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Cybersecurity issues are addressed in the development of a critical infrastructure and key resources protection plan.*
(2) *Data privacy issues are addressed in the development of a critical infrastructure and key resources protection plan.*
(3) *Business Continuity & Disaster Recovery (BC/DR) operations are conducted according to documented policies, standards, procedures and/or other entity directives.*
(4) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support Business Continuity & Disaster Recovery (BC/DR) operations.*
(5) *Responsibility and authority for the performance of Business Continuity & Disaster Recovery (BC/DR)-related activities are assigned to designated personnel.*

11.4.1 Recovery Time / Point Objectives (RTO / RPO)

The entity must facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

Relevant SCF Control(s):
- BCD-01.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Time period consistent with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for the recovery of the system is determined.*
(2) *The alternate storage site is configured to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).*

11.4.2 Recovery Operations Criteria

The entity must define specific criteria that must be met to initiate Business Continuity / Disaster Recover (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

Relevant SCF Control(s):

- BCD-01.5

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Criteria that must be met to initiate Business Continuity / Disaster Recovery (BC/DR) plans that facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) is defined.*

11.4.3 Identify Critical Assets

The entity must identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.

Relevant SCF Control(s):

- BCD-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions are identified.

(2) Critical TAASD supporting entity-defined criteria mission and business functions are identified.

11.4.4 Resume All Missions & Business Functions

The entity must resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.

Relevant SCF Control(s):

- BCD-02.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The contingency plan activation time period within which to resume all mission and business functions is defined.

(2) The resumption of all mission and business functions are planned for within an entity-defined time period of contingency plan activation.

11.4.5 Continue Essential Mission & Business Functions

The entity must 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.

Relevant SCF Control(s):

- BCD-02.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The continuance of entity-defined criteria mission and business functions with minimal or no loss of operational continuity is planned for.

11.4.6 Resume Essential Missions & Business Functions

The entity must resume essential missions and business functions within an entity-defined time period of contingency plan activation.

Relevant SCF Control(s):
- BCD-02.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The contingency plan activation time period within which to resume essential mission and business functions is defined.

(2) The resumption of essential mission and business functions are planned for within an entity-defined time period of contingency plan activation.

11.4.7 Data Backups

The entity must create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).

Relevant SCF Control(s):
- BCD-11

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The confidentiality of backup sensitive and/or regulated data is protected at storage locations.

11.4.8 Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution

The entity must ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.

Relevant SCF Control(s):
- BCD-12

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Secure baseline configurations exist for systems, applications and/or services protect the confidentiality and integrity of data being stored, processed and/or transmitted.

(2) Systems, applications and/or services are securely recovered / reconstituted to a known, trusted state after a disruption, compromise or failure.

11.5 Capacity & Performance Planning

The entity must 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.

Relevant SCF Control(s):
- CAP-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Resources to be allocated to protect the availability of resources are defined.

(2) Capacity & performance planning operations are conducted according to documented policies, standards, procedures and/or other entity directives.

(3) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support capacity & performance planning operations.

(4) *Responsibility and authority for the performance of capacity & performance planning-related activities are assigned to designated personnel.*

11.5.1 Capacity & Performance Management

The entity must facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.

Relevant SCF Control(s):
- CAP-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Resources to be allocated to protect the availability of resources are defined.*
(2) *Capacity & performance planning operations are conducted according to documented policies, standards, procedures and/or other entity directives.*
(3) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support capacity & performance planning operations.*
(4) *Responsibility and authority for the performance of capacity & performance planning-related activities are assigned to designated personnel.*

11.5.2 Capacity Planning

The entity must conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.

Relevant SCF Control(s):
- CAP-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Capacity planning is conducted so that the necessary capacity exists during contingency operations for information processing.*

11.5.3 Elastic Expansion

The entity automatically scales the resources available for Technology Assets, Applications and/or Services (TAAS), as demand conditions change.

Relevant SCF Control(s):
- CAP-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Applicable services are configured to dynamically expand the resources available for services, as demand conditions change.*

11.6 Change Management

The entity must 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.

Relevant SCF Control(s):
- CHG-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Configuration change control activities are coordinated and overseen by entity-defined configuration change control element.*
(2) *Configuration change decisions associated with the system are documented.*
(3) *Approved configuration-controlled changes to the system are implemented.*
(4) *Change management operations are conducted according to documented policies, standards, procedures and/or other directives.*
(5) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support change management operations.*
(6) *Responsibility and authority for the performance of change management-related activities are assigned to designated personnel.*

11.6.1 Configuration Change Control

The entity must govern the technical configuration change control processes.

Relevant SCF Control(s):
- CHG-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Changes to the system are:*
    a. *Reviewed; and*
    b. *Approved or disapproved.*
(2) *Approved configuration-controlled changes to the system are implemented.*

11.6.2 Prohibition Of Changes

The entity must prohibit unauthorized changes, unless entity-approved change requests are received.

Relevant SCF Control(s):
- CHG-02.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Mechanisms used to automate configuration change control are defined.*
(2) *Entity-defined automated mechanisms are used to prohibit changes to the system until designated approvals are received.*

11.6.3 Security Impact Analysis for Changes

The entity must analyze proposed changes for potential security impacts, prior to the implementation of the change.

Relevant SCF Control(s):
- CHG-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Proposed configuration-controlled changes to the system are reviewed with explicit consideration for security impacts.*

11.7 Cloud Security

The entity must 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.

Relevant SCF Control(s):
- CLD-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The entity facilitates the implementation of cloud management controls to ensure cloud instances are securely configured and maintained.
(2) Cloud management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(3) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support cloud management operations.
(4) Responsibility and authority for the performance of cloud management-related activities are assigned to designated personnel.

11.7.1 Cloud Services

The entity must facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.

Relevant SCF Control(s):

- CLD-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The entity facilitates the implementation of cloud management controls to ensure cloud instances are securely configured and maintained.
(2) Cloud management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(3) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support cloud management operations.
(4) Responsibility and authority for the performance of cloud management-related activities are assigned to designated personnel.

11.7.2 Cloud Security Architecture

The entity must ensure the cloud security architecture supports the entity's technology strategy to securely design, configure and maintain cloud employments.

Relevant SCF Control(s):

- CLD-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A cloud security architecture is defined to address cloud employments that support the entity's mission.
(2) The cloud security architecture supports the entity's technology strategy to securely design, configure and maintain cloud employments.

11.7.3 Geolocation Requirements for Processing, Storage and Service Locations

The entity must control the location of cloud processing/storage based on business requirements that includes statutory, regulatory and contractual obligations.

Relevant SCF Control(s):

- CLD-09

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Locations where information processing and data storage is/are to be restricted are defined.
(2) Requirements or conditions for restricting the location of information processing, information storage or information services are defined.

(3) *Based on requirements, information processing, information storage or information services is/are restricted to locations.*

11.7.4 Sensitive Data In Public Cloud Providers

The entity must limit and manage the storage of sensitive and/or regulated data in public cloud providers.

Relevant SCF Control(s):
- CLD-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Sensitive and/or regulated data in public cloud providers is identified and documented.
(2) The storage of sensitive and/or regulated data in public cloud providers is controlled.

11.8 Compliance

The entity must ensure controls are in place to ensure adherence to applicable statutory, regulatory and contractual compliance obligations, as well as internal company standards.

Relevant SCF Control(s):
- CPL-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) The entity analyzes its business practices to determine applicable statutory, regulatory and/or contractual obligations.
(2) Compliance management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(3) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support compliance management operations.
(4) Responsibility and authority for the performance of compliance management-related activities are assigned to designated personnel.

11.8.1 Statutory, Regulatory & Contractual Compliance

The entity must facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.

Relevant SCF Control(s):
- CPL-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) The entity analyzes its business practices to determine applicable statutory, regulatory and/or contractual obligations.
(2) Compliance management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(3) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support compliance management operations.
(4) Responsibility and authority for the performance of compliance management-related activities are assigned to designated personnel.

11.8.2 Compliance Scope

The entity must document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.

Relevant SCF Control(s):
- CPL-01.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The entity's applicable cybersecurity and data protection controls are determined through the analysis of business practices to determine required statutory, regulatory and/or contractual compliance obligations.

(2) A recurring process exists to validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.

11.9 Configuration Management

The entity must 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.

Relevant SCF Control(s):

- CFG-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The scope for the configuration management plan is entity-wide.

(2) The types of changes to the system that are configuration-controlled are defined.

(3) A configuration management plan for systems, applications and services is:

a. Developed;

b. Documented; and

c. Implemented.

(4) Configuration management operations are conducted according to documented policies, standards, procedures and/or other entity directives.

(5) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support configuration management operations.

(6) Responsibility and authority for the performance of configuration management-related activities are assigned to designated personnel.

11.9.1 Secure Baseline Configurations

The entity must develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.

Relevant SCF Control(s):

- CFG-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A current baseline configuration for systems, applications and services is developed and documented.

(2) The baseline configuration includes hardware, software, firmware and documentation.

(3) Security configuration settings for information technology products employed in the system are enforced.

(4) The baseline configuration is maintained (reviewed / updated) throughout the system development life cycle under configuration control.

(5) Configuration settings that reflect the most restrictive mode consistent with operational requirements are established and documented for components employed within the system using entity-defined common secure configurations.

11.9.2 Approved Configuration Deviations

The entity must document, assess risk and approve or deny deviations to standardized configurations.

Relevant SCF Control(s):

- CFG-02.7

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) 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.
(2) Changes to the configuration settings are controlled in accordance with the entity's policies and procedures.
(3) Any deviations from established configuration settings are identified and documented.
(4) Any deviations from established configuration settings are approved.
(5) Common secure configurations to establish and document configuration settings for components employed within the system are defined.

11.9.3 LEAST FUNCTIONALITY

The entity must configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols and/or services.

Relevant SCF Control(s):
- CFG-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Configuration settings for the system that reflect the most restrictive mode consistent with operational requirements are defined (e.g., principle of least functionality).
(2) Systems are configured to provide only the defined essential capabilities, where unnecessary or nonsecure functions, ports, protocols, connections and services are disabled or removed.

11.10 CONTINUOUS MONITORING

The entity must 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 entity will have "blind spots" in its situational awareness that could lead to system compromise, data exfiltration, or unavailability of needed computing resources.

Relevant SCF Control(s):
- MON-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The continuous monitoring program is entity-wide.
(2) Monitoring objectives to detect attacks and indicators of potential attacks on the system are defined.
(3) Techniques and methods used to identify unauthorized use of the system are defined.
(4) Event monitoring operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(5) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support event monitoring operations.
(6) Responsibility and authority for the performance of event monitoring-related activities are assigned to designated personnel.

11.10.1 AUTOMATED TOOLS FOR REAL-TIME ANALYSIS

The entity must utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.

Relevant SCF Control(s):
- MON-01.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Automated tools and mechanisms are employed to support a near real-time analysis of events.

11.10.2 System Generated Alerts

The entity must generate, monitor, correlate and respond to alerts from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.

Relevant SCF Control(s):
- MON-01.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Audit records contain information that establishes what type of event occurred.
(2) Audit records for the selected event types and audit record content are generated.
(3) Personnel or roles to be alerted when indications of compromise or potential compromise occur is/are defined.
(4) Compromise indicators are defined.
(5) Personnel or roles are alerted when system-generated compromise indicators occur.

11.10.3 Security Event Monitoring

The entity must review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.

Relevant SCF Control(s):
- MON-01.8

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The frequency at which system audit records are reviewed and analyzed is defined.
(2) System audit records are reviewed and analyzed per an entity-defined frequency for indications and the potential impact of inappropriate or unusual activity.
(3) Response actions to system security alerts and advisories are identified.
(4) System security alerts and advisories are monitored.
(5) Actions in response to system security alerts and advisories are taken.
(6) The event types selected for logging are reviewed per an entity-defined frequency.
(7) System audit records are reviewed and analyzed per an entity-defined frequency for indications and the potential impact of inappropriate or unusual activity.

11.10.4 Content of Event Logs

The entity must configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:

(1) Establish what type of event occurred;
(2) When (date and time) the event occurred;
(3) Where the event occurred;
(4) The source of the event;
(5) The outcome (success or failure) of the event; and
(6) The identity of any user/subject associated with the event.

Relevant SCF Control(s):
- MON-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The content of audit records needed to support monitoring, analysis, investigation and reporting of unlawful or unauthorized system activity is defined.
(2) Audit records contain information that establishes:
    a. What type of event occurred;

b. *When the event occurred;*
c. *Where the event occurred;*
d. *The source of the event;*
e. *The outcome of the event; and*
f. *The identity of the individuals, subjects, objects, or entities associated with the event.*

(3) *The event types selected for logging are updated per an entity-defined frequency.*

11.10.5 Monitoring for Indicators of Compromise (IOC)

The entity must identify and alert on Indicators of Compromise (IoC).

Relevant SCF Control(s):
- MON-11.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Anomalous or suspicious behavior is defined.*
(2) *Indicators of Compromise (IOC) are defined.*
(3) *Sources that provide IOC are defined.*
(4) *IOC provided by sources are:*
   a. *Discovered; and*
   b. *collected.*
(5) *Unauthorized use of the system is identified through techniques and methods.*

11.10.6 Anomalous Behavior

The entity must utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.

Relevant SCF Control(s):
- MON-16

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Environments or resources which may contain or may be related to anomalous or suspected adversarial behavior are defined.*
(2) *Systems are monitored to detect unauthorized:*
   a. *Local connections;*
   b. *Network connections; and*
   c. *Remote connections.*
(3) *Outbound communications traffic at the external interfaces to the system is analyzed to discover anomalies.*
(4) *Outbound communications traffic at interior points is analyzed to discover anomalies.*
(5) *Anomalous or suspected adversarial behavior in or related to entity-defined environments or resources are analyzed.*
(6) *Unauthorized use of the system is identified.*
(7) *Anomalous or suspicious behavior is defined.*
(8) *Personnel or roles to report atypical usage is/are defined.*
(9) *Atypical usage of system accounts is reported to entity-defined personnel or roles.*

11.11 Cryptographic Protections

The entity must ensure the confidentiality and integrity of its data through implementing appropriate cryptographic technologies to protect systems, applications, services and data.

Relevant SCF Control(s):
- CRY-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Cryptographic uses are:
  a. Identified; and
  b. Defined.
(2) Cryptographic mechanisms intended to prevent unauthorized disclosure of sensitive and/or regulated data are identified.
(3) Entity-defined types of cryptography are implemented to protect the confidentiality of sensitive and/or regulated data.
(4) Cryptographic protections management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(5) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support cryptographic protections management operations.
(6) Responsibility and authority for the performance of cryptographic protections management-related activities are assigned to designated personnel.

11.11.1 Transmission Confidentiality

The entity must use cryptographic mechanisms to protect the confidentiality of data being transmitted.

Relevant SCF Control(s):
- CRY-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The types of cryptography for protecting the confidentiality of data are defined.
(2) Cryptographic mechanisms are implemented to prevent the unauthorized disclosure of data during transmission.
(3) Entity-defined types of cryptography are implemented to protect the confidentiality of sensitive and/or regulated data.

11.11.2 Encrypting Data At Rest

The entity must use cryptographic mechanisms to prevent unauthorized disclosure of data at rest.

Relevant SCF Control(s):
- CRY-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The confidentiality of sensitive and/or regulated data stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.
(2) Cryptographic mechanisms are implemented to prevent the unauthorized disclosure of sensitive and/or regulated data while in storage.

11.11.3 Public Key Infrastructure (PKI)

The entity must securely implement an internal Public Key Infrastructure (PKI) infrastructure or obtain PKI services from a reputable PKI service provider.

Relevant SCF Control(s):
- CRY-08

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Requirements for key generation, distribution, storage, access and destruction are defined.
(2) A certificate policy for issuing public key certificates is defined.
(3) Public key certificates are issued under an entity-defined certificate policy or public key certificates are obtained from an approved service provider.

11.11.4 Cryptographic Key Management

The entity must facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.

Relevant SCF Control(s):
- CRY-09

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Requirements for key generation, distribution, storage, access and destruction are defined.
(2) Protected storage for cryptographic keys is provided using entity-defined criteria.
(3) Cryptographic keys are established in the system in accordance with entity-defined key management requirements.
(4) Cryptographic keys are managed in the system in accordance with entity-defined key management requirements.

11.12 Data Classification & Handling

The entity must ensure that technology assets, both electronic and physical, are properly classified and measures implemented to protect the entity'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.

Relevant SCF Control(s):
- DCH-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Paper media containing sensitive and/or regulated data is physically controlled.
(2) Digital media containing sensitive and/or regulated data is physically controlled.
(3) Data classification & handling management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(4) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support data classification & handling management operations.
(5) Responsibility and authority for the performance of data classification & handling management-related activities are assigned to designated personnel.

11.12.1 Sensitive and/or Regulated Data Protection

The entity must protect sensitive and/or regulated data wherever it is processed and/or stored.

Relevant SCF Control(s):
- DCH-01.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Sensitive and/or regulated data inventories exist.
(2) Protection mechanisms are defined for each type of sensitive and/or regulated data.
(3) Entity-defined mechanisms protect sensitive and/or regulated data wherever it is stored.

11.12.2 Defining Access Authorizations for Sensitive and/or Regulated Data

The entity must explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive and/or regulated data.

Relevant SCF Control(s):
- DCH-01.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Specific individuals and/or roles for logical and /or physical access to sensitive and/or regulated data are defined.

(2) *Only authorized individuals are provided logical and /or physical access to sensitive and/or regulated data.*

11.12.3 Data & Asset Classification

The entity must ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.

Relevant SCF Control(s):
- DCH-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *A data classification scheme is defined that covers reasonable data types to address the entity's operational needs.*
(2) *Data and assets are categorized in accordance with the data classification scheme that addresses applicable statutory, regulatory and contractual requirements.*

11.12.4 Sensitive Data Inventories

The entity must maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.

Relevant SCF Control(s):
- DCH-06.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *An inventory is maintained for all sensitive and/or regulated data.*
(2) *Recurring inventories keep sensitive and/or regulated data inventories current and accurate.*

11.12.5 Use of External Technology Assets, Applications and/or Services (TAAS)

The entity must govern how external parties, including Technology Assets, Applications and/or Services (TAAS), are used to securely store, process and transmit data.

Relevant SCF Control(s):
- DCH-13

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Connections to external systems are:*
    a. *Identified;*
    b. *Verified; and*
    c. *Controlled/limited.*
(2) *The use of external systems:*
    a. *Identified;*
    b. *Verified; and*
    c. *Controlled/limited.*

11.12.6 Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS)

The entity must ensure that the requirements for the protection of sensitive/regulated data processed, stored or transmitted on external Technology Assets, Applications and/or Services (TAAS), are implemented in accordance with applicable statutory, regulatory and contractual obligations.

Relevant SCF Control(s):
- DCH-13.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *The frequency at which to review / update the procedures is defined.*
(2) *Entity controls ensure that requirements for the protection of sensitive and/or regulated information that is processed, stored or transmitted on external systems are implemented in accordance with applicable laws, executive orders, directives, policies, regulations and standards.*
(3) *Procedures are established to ensure that requirements for the protection of sensitive and/or regulated information that is processed, stored or transmitted on external systems are implemented in accordance with applicable laws, executive orders, directives, policies, regulations and standards.*
(4) *Procedures are reviewed / updated frequently.*

11.12.7 Media & Data Retention

The entity must retain media and data in accordance with applicable statutory, regulatory and contractual obligations.

Relevant SCF Control(s):
- DCH-18

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *The frequency with which to conduct reviews of persistent the entity's storage locations is defined.*
(2) *Persistent the entity's storage locations are identified.*
(3) *Reviews of persistent the entity's storage locations are conducted per an entity-defined frequency to identify sensitive / regulated data that is no longer needed.*
(4) *Sensitive / regulated data that is no longer needed is removed.*

11.12.8 Geographic Location of Data

The entity must 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.

Relevant SCF Control(s):
- DCH-19

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Locations where information processing and data storage is/are to be restricted are defined.*
(2) *Requirements or conditions for restricting the location of information processing, information storage or information services are defined.*
(3) *Based on requirements, information processing, information storage or information services is/are restricted to locations.*

11.12.9 Information Disposal

The entity must securely dispose of, destroy or erase information.

Relevant SCF Control(s):
- DCH-21

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Techniques used to dispose of, destroy and/or erase information following the retention period are defined.*
(2) *Entity-defined techniques are used to dispose of, destroy and/or erase following the retention period.*

11.12.10 Information Location

The entity must identify and document the location of information and the specific system components on which the information resides.

Relevant SCF Control(s):

- DCH-24

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Information for which the location is to be identified and documented is defined.
(2) The location of sensitive / regulated data is identified and documented.
(3) The specific system components on which entity-defined information is processed are identified and documented.
(4) The specific system components on which entity-defined information is stored are identified and documented.
(5) Changes to the location (e.g., system or system components) where entity-defined information is processed are documented.
(6) Changes to the location (e.g., system or system components) where entity-defined information is stored are documented.

11.12.11 Transfer of Sensitive and/or Regulated Data

The entity must restrict and govern the transfer of sensitive and/or regulated data to third-countries or international entities.

Relevant SCF Control(s):
- DCH-25

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The statutory, regulatory and/or contractual basis restricts the transfer of sensitive and/or regulated data to third-countries or international entities is identified.
(2) Mechanisms to restrict the transfer of sensitive and/or regulated data to third-countries or international entities are:
  a. Defined; and
  b. Implemented.

11.12.12 Ad-Hoc Transfers

The entity must secure ad-hoc exchanges of large digital files with internal or external parties.

Relevant SCF Control(s):
- DCH-17

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Ad-hoc exchanges of large digital files with internal or external parties are secured according to entity-defined protection criteria.

11.13 Embedded Technology

The entity must 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.

Relevant SCF Control(s):
- EMB-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Embedded technology controls are implemented to protect the:
  a. Confidentiality of IoT and/or OT technologies;
  b. Integrity of IoT and/or OT technologies;
  c. Availability of IoT and/or OT technologies; and
  d. Safety of IoT and/or OT technologies.

(2) *Embedded technology management operations are conducted according to documented policies, standards, procedures and/or other entity directives.*
(3) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support embedded technology management operations.*
(4) *Responsibility and authority for the performance of embedded technology management-related activities are assigned to designated personnel.*

11.13.1 Prevent Alterations

The entity must protect embedded devices by preventing the unauthorized installation and execution of software.

Relevant SCF Control(s):
- EMB-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Embedded devices are protected by preventing the unauthorized installation and execution of software.*

11.13.2 Embedded Technology Maintenance

The entity must protect securely update software and upgrade functionality on embedded devices.

Relevant SCF Control(s):
- EMB-07

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Embedded devices are capable of securely receiving software updates and upgraded functionality.*

11.13.3 Embedded Technology Reviews

The entity must 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.

Relevant SCF Control(s):
- EMB-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Deployed embedded technologies are evaluated per an entity-defined interval (no less than annually) to ensure that necessary updates to mitigate the risks associated with legacy embedded technologies are identified and implemented.*

11.14 Endpoint Security

The entity must 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.

Relevant SCF Control(s):
- END-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Security configuration settings for information technology products employed in the system are established and included in the baseline configuration.*
(2) *Endpoint security management operations are conducted according to documented policies, standards, procedures and/or other entity directives.*

(3) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support endpoint security management operations.*
(4) *Responsibility and authority for the performance of endpoint security management-related activities are assigned to designated personnel.*

11.14.1 Endpoint Protection Measures

The entity must protect the confidentiality, integrity, availability and safety of endpoint devices.

Relevant SCF Control(s):
- END-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *The confidentiality and integrity of sensitive / regulated data at rest is protected.*

11.14.2 Malicious Code Protection (Anti-Malware)

The entity must utilize antimalware technologies to detect and eradicate malicious code.

Relevant SCF Control(s):
- END-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) The frequency for malicious code scans is defined.
(2) Malicious code scans are performed with the defined frequency.
(3) Malicious code protection mechanisms are configured to perform real-time scans of files from external sources as the files are downloaded, opened or executed.
(4) Designated locations for malicious code protection are identified.
(5) Protection from malicious code at designated locations is provided.

11.14.3 Always On Protection

The entity must 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.

Relevant SCF Control(s):
- END-04.7

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Malicious code protection mechanisms are configured to perform:
  a. Real-time scans of files from external sources as the files are downloaded, opened or executed; and
  b. Scans of the system per an entity-defined frequency.
(2) Real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

11.14.4 Phishing & Spam Protection

The entity must utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.

Relevant SCF Control(s):
- END-08

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Spam and/or phishing protection mechanisms are employed at system entry points to:

a. *Detect unsolicited / potentially harmful messages; and*
b. *Act on unsolicited / potentially harmful messages.*

11.15 HUMAN RESOURCES SECURITY

The entity must create a cybersecurity and data protection-minded workforce and an environment that is conducive to innovation, considering issues such as culture, reward and collaboration.

Relevant SCF Control(s):
- HRS-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Personnel security procedures to facilitate the implementation of the personnel security policy and associated personnel security controls are developed and documented.
(2) An official to manage the personnel security policy and procedures is defined.
(3) Personnel management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(4) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support personnel management operations.
(5) Responsibility and authority for the performance of personnel management-related activities are assigned to designated personnel.

11.15.1 ONBOARDING, TRANSFERRING & OFFBOARDING PERSONNEL

The entity must define cybersecurity roles & responsibilities for all personnel.

Relevant SCF Control(s):
- HRS-01.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The entity proactively governs secure practices to address personnel onboarding, transfers and offboarding actions

11.15.2 DEFINED ROLES & RESPONSIBILITIES

The entity must define cybersecurity roles & responsibilities for all personnel.

Relevant SCF Control(s):
- HRS-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Cybersecurity and data protection roles and responsibilities are incorporated into the entity's position descriptions.

11.15.3 COMPETENCY REQUIREMENTS FOR SECURITY-RELATED POSITIONS

The entity must ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.

Relevant SCF Control(s):
- HRS-03.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Defined competency requirements ensure that all cybersecurity and data protection-related positions are staffed by qualified individuals who have the necessary skill set.

11.15.4 PERSONNEL SCREENING

The entity must manage personnel security risk by screening individuals prior to authorizing access.

Relevant SCF Control(s):
- HRS-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Conditions that require the rescreening of individuals are defined.
(2) The frequency of rescreening individuals where it is so indicated is defined.
(3) Individuals are screened prior to authorizing access to the system.
(4) Individuals are rescreened in accordance with entity-defined conditions.

11.15.5 Roles With Special Protection Measures

The entity must ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy entity-defined personnel screening criteria.

Relevant SCF Control(s):
- HRS-04.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Enhanced personnel screening for individuals is defined.
(2) The frequency with which to reassess individual positions and access to sensitive / regulated data is defined.
(3) Individuals that require enhanced personnel screening are identified.
(4) Positions that require access to sensitive / regulated data are identified.
(5) Enhanced personnel screening is conducted for individuals.

11.15.6 Terms of Employment

The entity must require all employees and contractors to apply cybersecurity and data protection principles in their daily work.

Relevant SCF Control(s):
- HRS-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Through terms of employment, all employees and contractors are required to apply cybersecurity and data protection principles in their daily work.
(2) Rules are provided to individuals who require access to the system.

11.15.7 Rules of Behavior

The entity must define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.

Relevant SCF Control(s):
- HRS-05.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Rules that describe responsibilities and expected behavior for system usage and protecting sensitive / regulated data are established.
(2) Before authorizing access to information and the system, a documented acknowledgement from such individuals indicating that they have read, understand and agree to abide by the rules of behavior is received.
(3) The frequency at which the rules of behavior are reviewed and updated is defined.
(4) The rules of behavior are reviewed / updated per an entity-defined frequency.
(5) The frequency for individuals to read and re-acknowledge the rules of behavior is defined.

(6) *Individuals who have acknowledged a previous version of the rules of behavior are required to read and reacknowledge the entity's current rules of behavior.*

11.15.8 Policy Familiarization & Acknowledgement

The entity must ensure personnel receive recurring familiarization with the entity's cybersecurity and data protection policies and provide acknowledgement.

Relevant SCF Control(s):
- HRS-05.7

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Personnel receive recurring familiarization with the entity's cybersecurity / data privacy policies.*
(2) *A documented acknowledgement from individuals indicating that they have read, understand and agree to abide by the rules of behavior is received before authorizing access to sensitive / regulated data and the system.*

11.15.9 Personnel Sanctions

The entity must sanction personnel failing to comply with established security policies, standards and procedures.

Relevant SCF Control(s):
- HRS-07

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *A formal sanctions process is employed for individuals failing to comply with established cybersecurity / data privacy policies and procedures.*
(2) *Criteria and/or process for terminating system access authorization and any credentials coincide with personnel actions is established.*
(3) *Personnel or roles to be notified when a formal employee sanctions process is initiated is/are defined.*
(4) *The time period within which entity-defined personnel or roles must be notified when a formal employee sanctions process is initiated is defined.*
(5) *Personnel or roles is/are notified within an entity-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.*

11.15.10 Workplace Investigations

The entity must conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.

Relevant SCF Control(s):
- HRS-07.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Individuals with access to sensitive / regulated data are identified.*
(2) *Adverse information about individuals with access to sensitive / regulated data is defined.*
(3) *Entity systems to which individuals have access are identified.*
(4) *Mechanisms are in place to protect the entity's systems if adverse information develops or is obtained about individuals with access to sensitive / regulated data.*

11.15.11 Personnel Transfer

The entity must adjust logical and physical access authorizations to Technology Assets, Applications and/or Services (TAAS) and facilities upon personnel reassignment or transfer, in a timely manner.

Relevant SCF Control(s):
- HRS-08

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Criteria and/or process for terminating system access authorization and any credentials coincide with personnel actions is established.
(2) System access and credentials are terminated consistent with personnel actions such as termination or transfer.
(3) The system is protected during and after personnel transfer actions.

11.15.12 Personnel Termination

The entity must govern the termination of individual employment.

Relevant SCF Control(s):

- HRS-09

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Criteria and/or process for terminating system access authorization and any credentials coincide with personnel actions is established.
(2) System access and credentials are terminated consistent with personnel actions such as termination or transfer.
(3) The system is protected during and after personnel transfer actions.

11.15.13 Third-Party Personnel

The entity must govern third-party personnel by reviewing and monitoring third-party cybersecurity and data protection roles and responsibilities.

Relevant SCF Control(s):

- HRS-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Personnel or roles to be notified of any personnel transfers or terminations of external personnel who possess the entity's credentials and/or badges or who have system privileges is/are defined.
(2) Time period within which third-party providers are required to notify entity-defined personnel or roles of any personnel transfers or terminations of external personnel who possess the entity's credentials and/or badges or who have system privileges is defined.
(3) Personnel security requirements are established, including security roles and responsibilities for external providers.
(4) External providers are required to comply with personnel security policies and procedures established by the entity.
(5) Personnel security requirements are documented.
(6) External providers are required to notify personnel or roles of any personnel transfers or terminations of external personnel who possess the entity's credentials and/or badges or who have system privileges within an entity-defined time period.
(7) Provider compliance with personnel security requirements is monitored.

11.15.14 Identifying Authorized Work Locations

The entity must identify and document authorized working locations, including:

(1) Designated on-premises, entity-controlled work locations; and
(2) Other off-premises locations not under entity-control (e.g., work from home).

Relevant SCF Control(s):

- HRS-14

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Authorized working locations which are not on entity-controlled premises are defined.

11.16 Identification & Authentication

The entity must implement the concept of "least privilege" through limiting access to the entity's systems and data to authorized users only.

Relevant SCF Control(s):
- IAC-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A capability to govern logical identification and access management controls is implemented.
(2) The Identity & Access Management (IAM) program is entity-wide.
(3) IAM operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(4) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support IAM operations.
(5) Responsibility and authority for the performance of IAM-related activities are assigned to designated personnel.

11.16.1 Authenticate, Authorize and Audit (AAA)

The entity must strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).

Relevant SCF Control(s):
- IAC-01.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Access to the system is authorized based on a valid access authorization.
(2) System users are uniquely identified.
(3) System users are authenticated.
(4) An inventory of Authenticate, Authorize and Audit (AAA) solutions exists, including instances on-premises and hosted by an External Service Provider (ESP).
(5) Procedures exist to govern on-premises Authenticate, Authorize and Audit (AAA) solutions by assigned stakeholders.
(6) Contracts with ESP contain explicit governance requirements for ESP-controlled AAA solutions.

11.16.2 User & Service Account Inventories

The entity must maintain a current list of authorized users and service accounts.

Relevant SCF Control(s):
- IAC-01.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A current list of authorized users and services is maintained.

11.16.3 Multi-Factor Authentication (MFA)

The entity must use automated mechanisms to enforce Multi-Factor Authentication (MFA) for:

(1) Remote network access;
(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or
(3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.

Relevant SCF Control(s):
- IAC-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *MFA for access to privileged accounts is implemented.*
(2) *MFA for access to non-privileged accounts is implemented.*

11.16.4 User Provisioning & De-Provisioning

The entity must utilize a formal user registration and de-registration process that governs the assignment of access rights.

Relevant SCF Control(s):
- IAC-07

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *The validation and verification of identity evidence is conducted in person before a designated registration authority.*
(2) *Authorization is received from the entity's personnel or roles to assign an individual, group, role, service, or device identifier.*
(3) *In accordance with the entity's policy, procedures, prerequisites and criteria, system accounts:*
    a. *Created;*
    b. *Enabled;*
    c. *Modified;*
    d. *Disabled; and*
    e. *Removed.*

11.16.5 Role-Based Access Control (RBAC)

The entity must enforce a Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.

Relevant SCF Control(s):
- IAC-08

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *The entity implements a role-based access scheme or an attribute-based access scheme.*
(2) *Privileged user accounts are established and administered in accordance with entity-defined parameters.*
(3) *Access to sensitive and/or regulated data requiring special protection is granted only to individuals who:*
    a. *Have a valid access authorization that is demonstrated by assigned duties.*
    b. *Satisfy associated personnel security criteria.*

11.16.6 Authenticator Management

The entity must:
(1) Securely manage authenticators for users and devices; and
(2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.

Relevant SCF Control(s):
- IAC-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *The number of generations during which a password cannot be reused is specified.*
(2) *Reuse of passwords is prohibited during the specified number of generations.*
(3) *An immediate change to a permanent password is required when a temporary password is used for system logon.*
(4) *The frequency for changing or refreshing authenticators is defined.*
(5) *Events that trigger the change or refreshment of authenticators are defined.*
(6) *The identity of the individual, group, role, service, or device receiving the authenticator as part of the initial authenticator distribution is verified.*
(7) *Initial authenticator content for any authenticators issued by the entity is established.*

(8) *System authenticators are managed to ensure that authenticators have sufficient strength of mechanism for their intended use.*
(9) *System authenticators are managed through the establishment and implementation of administrative procedures for initial authenticator distribution. lost, compromised or damaged authenticators. and the revocation of authenticators.*
(10) *Default authenticators are changed at first use.*
(11) *Authenticators are changed or refreshed per an entity-defined frequency or when entity-defined events occur.*

11.16.7 Default Authenticators

The entity must ensure default authenticators are changed as part of account creation or system installation.

Relevant SCF Control(s):
- IAC-10.8

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Developers and installers of system components are required to provide unique authenticators or change default authenticators prior to delivery and installation.*

11.16.8 Password Managers

The entity must protect and store passwords via a password manager tool.

Relevant SCF Control(s):
- IAC-10.11

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Password managers are employed to generate and manage passwords.*

11.16.9 Account Management

The entity must proactively govern account management of individual, group, system, service, application, guest and temporary accounts.

Relevant SCF Control(s):
- IAC-15

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Criteria for account creation, enabling, modification, disabling and removal are defined.*
(2) *Approvals are required by entity-defined personnel or roles for requests to create accounts.*
(3) *Accounts are created in accordance with entity-defined policy, procedures, prerequisites and/or other criteria.*
(4) *Accounts are enabled in accordance with entity-defined policy, procedures, prerequisites and/or other criteria.*
(5) *Accounts are modified in accordance with entity-defined policy, procedures, prerequisites and/or other criteria.*
(6) *Accounts are disabled in accordance with entity-defined policy, procedures, prerequisites and/or other criteria.*
(7) *Accounts are removed in accordance with entity-defined policy, procedures, prerequisites and/or other criteria.*
(8) *The use of accounts is monitored.*
(9) *Accounts are reviewed for compliance with account management requirements entity-defined frequency.*
(10) *Account management processes are aligned with:*
    a. *Personnel termination processes; and*
    b. *Personnel transfer processes.*
(11) *Account managers and entity-defined personnel or roles are notified within an entity-defined time period when:*
    a. *Accounts are no longer required;*
    b. *Users are terminated or transferred; and*
    c. *System usage or the need to know changes for an individual.*

11.16.10 System Account Reviews

The entity must review all system accounts and disable any account that cannot be associated with a business process and owner.

Relevant SCF Control(s):
- IAC-15.7

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Access to the system is authorized based on entity-defined attributes (as required).

11.16.11 Privileged Account Management (PAM)

The entity must inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of the entity's management.

Relevant SCF Control(s):
- IAC-16.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) All privileged accounts are inventoried.

(2) Validation is performed for each person with elevated privileges for authorization by the appropriate level of the entity's management.

11.16.12 Privileged Account Inventories

The entity must restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).

Relevant SCF Control(s):
- IAC-16

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(3) Privileged access rights for users and services are:

a. Restricted based on roles; and

b. Controlled.

11.16.13 Periodic Review of Account Privileges

The entity must 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.

Relevant SCF Control(s):
- IAC-17

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The frequency at which to review the privileges assigned to roles or classes of users is defined.

(2) Roles or classes of users to which privileges are assigned are defined.

(3) The privileges assigned to roles or classes of users are reviewed per an entity-defined frequency to validate the need for such privileges.

(4) Privileges are reassigned or removed, as necessary.

11.16.14 Access Enforcement

The entity must enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."

Relevant SCF Control(s):

- IAC-20

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Approved authorizations for logical access to information and system resources are enforced in accordance with applicable access control policies.
(2) The principle of least privilege is employed, allowing only authorized access for users (or processes acting on behalf of users) that are necessary to accomplish assigned the entity's tasks.
(3) Authorized users are identified.
(4) Processes acting on behalf of authorized users are identified.
(5) Devices (including other systems) authorized to connect to the system are identified.
(6) System access is limited to:
    a. Authorized users;
    b. Processes acting on behalf of authorized users; and
    c. Authorized devices (including other systems).

11.16.15 Least Privilege

The entity must utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with the entity's business functions.

Relevant SCF Control(s):
- IAC-21

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Entity-defined systems or system components implement the security design principle of least privilege.
(2) Privileged accounts are identified.
(3) Access to privileged accounts is authorized in accordance with the principle of least privilege.
(4) Security functions are identified.
(5) Access to security functions is authorized in accordance with the principle of least privilege.

11.17 Incident Response

The entity must establish and maintain a viable and tested capability to respond to cybersecurity or data privacy-related incidents in a timely manner, where the entity's personnel understand how to detect and report potential incidents.

Relevant SCF Control(s):
- IRO-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The rigor of incident handling activities is comparable and predictable across the entity.
(2) The intensity of incident handling activities is comparable and predictable across the entity.
(3) The scope of incident handling activities is comparable and predictable across the entity.
(4) The results of incident handling activities are comparable and predictable across the entity.
(5) Incident handling activities are coordinated with contingency planning activities.
(6) Incident response management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(7) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support incident response management operations.
(8) Responsibility and authority for the performance of incident response management-related activities are assigned to designated personnel.

11.17.1 Incident Handling

The entity's incident handling processes cover:

(1) Preparation;
(2) Automated event detection or manual incident report intake;
(3) Analysis;
(4) Containment;
(5) Eradication; and
(6) Recovery.

Relevant SCF Control(s):
- IRO-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An incident handling capability for incidents is implemented that is consistent with the incident response plan.
(2) The incident handling capability includes:
  a. Preparation;
  b. Detection;
  c. Analysis;
  d. Containment;
  e. Eradication; and
  f. Recovery.
(3) Incident handling activities are coordinated with contingency planning activities.
(4) The operational incident-handling capability includes user response activities.

11.17.2 Indicators of Compromise (IOC)

The entity must define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.

Relevant SCF Control(s):
- IRO-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Anomalous or suspicious behavior is defined.
(2) Environments or resources which may contain or may be related to anomalous or suspected adversarial behavior are defined.
(3) Anomalous or suspected adversarial behavior in or related to entity-defined environments or resources are analyzed.
(4) Entity systems and system components are monitored on an ongoing basis for anomalous or suspicious behavior.

11.17.3 Incident Response Plan (IRP)

The entity must maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.

Relevant SCF Control(s):
- IRO-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Personnel or roles that review and approve the IRP is/are identified.
(2) Entities, personnel or roles with designated responsibility for incident response are defined.
(3) An IRP is developed that:
  a. Provides the entity with a roadmap for implementing its incident response capability;
  b. Describes the structure and entity of the incident response capability;
  c. Provides a high-level approach for how the incident response capability fits into the overall entity;
  d. Meets the unique requirements of the entity with regard to mission, size, structure and functions;
  e. Defines reportable incidents;
  f. Provides metrics for measuring the incident response capability within the entity;
  g. Defines the resources and management support needed to effectively maintain and mature an incident response capability;

h. Addresses the sharing of incident information;
i. Designates responsibilities to the entity's entities, personnel, or roles; and
j. Is reviewed and approved by personnel or roles frequency.

(4) Copies of the incident response plan are distributed to designated incident response personnel (identified by name or by role).

11.17.4 Integrated Security Incident Response Team (ISIRT)

The entity must establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.

Relevant SCF Control(s):
- IRO-07

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An integrated incident response team is established and maintained.
(2) The time period within which an integrated incident response team can be deployed is defined.
(3) The cyber incident response team can be deployed by the entity within an entity-defined time period.

11.17.5 Incident Stakeholder Reporting

The entity must timely-report incidents to applicable:

(1) Internal stakeholders;
(2) Affected clients & third-parties; and
(3) Regulatory authorities.

Relevant SCF Control(s):
- IRO-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The time period to report suspected incidents to the entity's incident response capability is defined.
(2) Authorities to whom incident information is to be reported are defined.
(3) Personnel are required to report suspected incidents to the entity's incident response capability within an entity-defined time period.
(4) Incident information is reported to entity-defined authorities.
(5) Suspected incidents are reported to the entity's incident response capability within an entity-defined time period.

11.17.6 Root Cause Analysis (RCA) & Lessons Learned

The entity must incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.

Relevant SCF Control(s):
- IRO-13

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An After Action Reviews (AARs), or a similar process, is conducted following incidents that require escalation to an Integrated Security Incident Response Team (ISIRT), or similar integrated team of cybersecurity, IT and business function representatives, are established to address a cybersecurity and/or data privacy incident response operations.
(2) Events that would require the current incident response policy / procedures to be reviewed / updated are defined.
(3) Incident response documentation is updated to address necessary changes to enable the timely and effective response to incidents.
(4) Events that initiate a review of the incident response training content are defined.

11.18 Information Assurance

The entity must ensure the adequacy of cybersecurity and data protection controls in development, testing and production environments.

Relevant SCF Control(s):

- IAO-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An Information Assurance (IA) process is implemented for conducting cybersecurity and data protection testing, training and monitoring activities associated with systems, applications and services.
(2) The Information Assurance Program (IAP) is entity-wide.
(3) The authorization processes are integrated into an entity-wide Risk Management Program (RMP).
(4) The cybersecurity and data protection security state of the entity's systems and the environments in which those systems operate are managed through authorization processes.
(5) Information assurance management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(6) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support information assurance management operations.
(7) Responsibility and authority for the performance of information assurance management-related activities are assigned to designated personnel.

11.18.1 Information Assurance Operations

The entity must facilitate the implementation of cybersecurity and data protection assessment and authorization controls.

Relevant SCF Control(s):

- IAO-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An Information Assurance (IA) process is implemented for conducting cybersecurity and data protection testing, training and monitoring activities associated with systems, applications and services.
(2) The Information Assurance Program (IAP) is entity-wide.
(3) The authorization processes are integrated into an entity-wide Risk Management Program (RMP).
(4) The cybersecurity and data protection security state of the entity's systems and the environments in which those systems operate are managed through authorization processes.
(5) Information assurance management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(6) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support information assurance management operations.
(7) Responsibility and authority for the performance of information assurance management-related activities are assigned to designated personnel.

11.18.2 Controls Assessments

The entity must formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) 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.

Relevant SCF Control(s):

- IAO-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The frequency at which to assess controls in the system and its environment of operation is defined.

(2) *Individuals or roles to whom control assessment results are to be provided are defined.*
(3) *Aan appropriate assessor or assessment team is selected for the type of assessment to be conducted.*
(4) *A control assessment plan is developed that describes the scope of the assessment, including:*
    a. *Controls and control enhancements under assessment;*
    b. *Assessment procedures to be used to determine control effectiveness;*
    c. *The assessment environment;*
    d. *The assessment team; and*
    e. *Assessment roles and responsibilities.*
(5) *The control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment.*

11.18.3 Security Assessment Report (SAR)

The entity must 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.

Relevant SCF Control(s):
- IAO-02.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *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.*

11.18.4 System Security & Privacy Plan (SSPP)

The entity must generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical Technology Assets, Applications and/or Services (TAAS), as well as influence inputs, entities and TAAS, providing a historical record of the data and its origins.

Relevant SCF Control(s):
- IAO-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *The system boundary is described and documented in the system security plan.*
(2) *The system components on which sensitive / regulated data is processed are identified and documented.*
(3) *The system components on which sensitive / regulated data is stored are identified and documented.*
(4) *Changes to the system or system component location where sensitive / regulated data is processed are documented.*
(5) *Changes to the system or system component location where sensitive / regulated data is stored are documented.*
(6) *A system security plan that describes specific threats to the system that are of concern to the entity is developed.*
(7) *A system security plan that describes the safeguards in place or planned for meeting the security requirements is developed.*
(8) *A system security plan that identifies individuals that fulfill system roles and responsibilities is developed.*
(9) *A system security plan that includes other relevant information necessary for the protection of sensitive / regulated data is developed.*
(10) *The system security plan is reviewed per an entity-defined frequency.*
(11) *The system security plan is protected from unauthorized disclosure.*

11.18.5 Threat Analysis & Flaw Remediation During Development

The entity requires system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan to identify and remediate flaws during development.

Relevant SCF Control(s):
- IAO-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The breadth of penetration testing is defined.
(2) The depth of penetration testing is defined.
(3) Constraints of penetration testing are defined.
(4) The developer of the system, system component, or system service is required to perform penetration testing:
    a. At an entity-defined breadth;
    b. At an entity-defined level of rigor; and
    c. Under entity-defined constraints.

11.18.6 Plan of Action & Milestones (POA&M)

The entity must generate a 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.

Relevant SCF Control(s):
- IAO-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Deficiencies and vulnerabilities to be addressed by the plan of action are identified.
(2) A plan of action is developed to document the planned remediation actions of the entity to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system.
(3) The frequency at which to update an existing plan of action based on the findings from control assessments, independent audits or reviews and continuous monitoring activities is defined.
(4) Existing plan of action is updated entity-defined frequency based on the findings from control assessments, independent audits or reviews and continuous monitoring activities.

11.18.7 Authorization To Operate (ATO)

The entity must ensure Technology Assets, Applications and/or Services (TAAS) are officially authorized prior to "go live" in a production environment.

Relevant SCF Control(s):
- IAO-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The frequency at which to assess controls in the system and its environment of operation is defined.
(2) Individuals or roles to whom control assessment results are to be provided are defined.
(3) An appropriate assessor or assessment team is selected for the type of assessment to be conducted.
(4) A control assessment plan is developed that describes the scope of the assessment, including controls and control enhancements under assessment.
(5) The control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment.
(6) Controls are assessed in the system and its environment of operation per an entity-defined 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 cybersecurity and data protection requirements.
(7) A control assessment report is produced that documents the results of the assessment.
(8) The results of the control assessment are provided to individuals or roles.

11.19 Maintenance

The entity must ensure that Technology Assets, Applications and/or Services (TAAS) are properly maintained to ensure continued performance and effectiveness. Maintenance processes apply additional scrutiny to the security of end-of-life or unsupported assets.

Relevant SCF Control(s):
- MNT-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A maintenance policy is developed and documented.
(2) The maintenance policy is disseminated to entity-defined personnel or roles.
(3) Maintenance procedures to facilitate the implementation of the maintenance policy and associated maintenance controls are developed and documented.
(4) The maintenance procedures are disseminated to entity-defined personnel or roles.
(5) Maintenance management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(6) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support maintenance management operations.
(7) Responsibility and authority for the performance of maintenance management-related activities are assigned to designated personnel.

11.19.1 Maintenance Operations

The entity must develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.

Relevant SCF Control(s):
- MNT-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A maintenance policy is developed and documented.
(2) The maintenance policy is disseminated to entity-defined personnel or roles.
(3) Maintenance procedures to facilitate the implementation of the maintenance policy and associated maintenance controls are developed and documented.
(4) The maintenance procedures are disseminated to entity-defined personnel or roles.
(5) Maintenance management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(6) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support maintenance management operations.
(7) Responsibility and authority for the performance of maintenance management-related activities are assigned to designated personnel.

11.19.2 Controlled Maintenance

The entity must conduct controlled maintenance activities throughout the lifecycle of the Technology Assets, Applications and/or Services (TAAS).

Relevant SCF Control(s):
- MNT-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Maintenance, repair and replacement of systems, applications and/or services are scheduled in accordance with manufacturer or vendor specifications and/or the entity's requirements.
(2) Approved configuration-controlled changes to the system are implemented.

11.19.3 Remote Maintenance

The entity must authorize, monitor and control remote, non-local maintenance and diagnostic activities.

Relevant SCF Control(s):
- MNT-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Nonlocal maintenance and diagnostic activities are:
   a. Approved; and
   b. Monitored.
(2) The use of nonlocal maintenance and diagnostic tools are allowed only as consistent with the entity's policy.

11.20 Mobile Device Management

The entity must govern risks associated with mobile devices, regardless of ownership (entity-owned, employee-owned or third-party owned). Wherever possible, technologies are employed to centrally manage mobile device access and data storage practices.

Relevant SCF Control(s):
- MDM-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Policies and standards facilitate the implementation of mobile device management controls.
(2) Usage restrictions are established for mobile devices.
(3) Mobile Device Management (MDM) operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(4) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support MDM operations.
(5) responsibility and authority for the performance of MDM-related activities are assigned to designated personnel.

11.20.1 Full Device & Container-Based Encryption

The entity must protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.

Relevant SCF Control(s):
- MDM-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Mobile devices on which to employ encryption are defined.
(2) Full-device or container-based encryption is implemented to protect the confidentiality of sensitive / regulated data on mobile devices.

11.20.2 Remote Purging

The entity must remotely purge selected information from mobile devices.

Relevant SCF Control(s):
- MDM-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Mobile devices to be purged or wiped of information are defined.
(2) Purging or wiping requirements and techniques to be used when mobile devices are purged or wiped of information are defined.
(3) Information is purged or wiped from entity-defined mobile devices based on entity-defined purging or wiping requirements or techniques after an entity-defined number consecutive, unsuccessful device logon attempts.

11.20.3 Personally-Owned Mobile Devices

The entity must restrict the connection of personally-owned, mobile devices to the entity's Technology Assets, Applications and/or Services (TAAS).

Relevant SCF Control(s):

- MDM-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The connection of personally-owned, mobile devices to entity systems and networks is restricted.

11.20.4 Organization-Owned Mobile Devices

The entity must prohibit the installation of non-approved applications or approved applications not obtained through the entity-approved application store.

Relevant SCF Control(s):

- MDM-07

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The installation of non-approved applications or approved applications not obtained through the entity-approved application store is prohibited.

11.20.5 Restricting Access To Authorized Technology Assets, Applications and/or Services (TAAS)

The entity must restrict the connectivity of unauthorized mobile devices from communicating with its Technology Assets, Applications and/or Services (TAAS).

Relevant SCF Control(s):

- MDM-11

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The connectivity of unauthorized mobile devices is restricted from communicating with systems, applications and services.

11.21 Network Security

The entity must ensure sufficient cybersecurity and data protection controls are architected to protect the confidentiality, integrity, availability and safety of the entity's network infrastructure, as well as to provide situational awareness of activity on the entity's networks.

Relevant SCF Control(s):

- NET-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) System and communications protection procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls are developed and documented.

(2) Network security management operations are conducted according to documented policies, standards, procedures and/or other entity directives.

(3) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support network security management operations.

(4) *Responsibility and authority for the performance of network security management-related activities are assigned to designated personnel.*

11.21.1 Layered Network Defenses

The entity must:

(1) Implement security functions as a layered structure that minimizes interactions between layers of the design; and
(2) Avoid any dependence by lower layers on the functionality or correctness of higher layers.

Relevant SCF Control(s):

- NET-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Security functions are implemented as a layered structure that minimizes interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

11.21.2 Guest Networks

The entity must implement and manage a secure guest network.

Relevant SCF Control(s):

- NET-02.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A secure guest network is:
  a. Defined; and
  b. Implemented

11.21.3 Boundary Protection

The entity must monitor and control communications at the external network boundary and at key internal boundaries within the network.

Relevant SCF Control(s):

- NET-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The external system boundary is defined.
(2) Key internal system boundaries are defined.
(3) Communications are protected at:
  a. The external system boundary; and
  b. Key internal boundaries.
(4) Communications are monitored at:
  a. The external system boundary; and
  b. Key internal boundaries.
(5) Communications are controlled at:
  a. The external system boundary; and
  b. Key internal boundaries.

11.21.4 Data Flow Enforcement – Access Control Lists (ACLs)

The entity must implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restricts network traffic to only what is authorized.

Relevant SCF Control(s):

- NET-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Information flow control policies are defined.
(2) Methods and enforcement mechanisms for controlling the flow of sensitive and/or regulated data are defined.
(3) Approved authorizations are enforced for controlling the flow of information within the system and between connected systems based on entity-defined information flow control policies.

11.21.5 Deny Traffic by Default & Allow Traffic by Exception

The entity must configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all, permit by exception).

Relevant SCF Control(s):
- NET-04.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Information flow control policies are defined.
(2) Methods and enforcement mechanisms for controlling the flow of sensitive / regulated data are defined.
(3) Approved authorizations are enforced for controlling the flow of information within the system and between connected systems based on entity-defined information flow control policies.

11.21.6 Domain Name Service (DNS) Resolution

The entity must ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.

Relevant SCF Control(s):
- NET-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Additional data origin authentication is provided along with the authoritative name resolution data that the system returns in response to external name/address resolution queries.
(2) Integrity verification artifacts are provided along with the authoritative name resolution data that the system returns in response to external name/address resolution queries.
(3) The means to indicate the security status of child zones (and if the child supports secure resolution services) is provided when operating as part of a distributed, hierarchical namespace.
(4) The means to enable verification of a chain of trust among parent and child domains when operating as part of a distributed, hierarchical namespace is provided.

11.21.7 Safeguarding Data Over Open Networks

The entity must implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.

Relevant SCF Control(s):
- NET-12

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Approved authorizations for logical access to information and system resources are enforced in accordance with applicable access control policies.

11.21.8 End-User Messaging Technologies

The entity must prohibit the transmission of unprotected sensitive/regulated data by end-user messaging technologies.

Relevant SCF Control(s):
- NET-12.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The transmission of unprotected sensitive / regulated data by end-user messaging technologies is prohibited through administrative and/or technical means.

11.21.9 Remote Access

The entity must define, control and review entity-approved, secure remote access methods.

Relevant SCF Control(s):
- NET-14

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Usage restrictions are established for each type of allowable remote system access.
(2) Types of allowable remote system access are defined.
(3) Connection requirements are established for each type of allowable remote system access.
(4) Each type of remote system access is authorized prior to establishing such connections.

11.21.10 Work From Anywhere (WFA) - Telecommuting Security

The entity must define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.

Relevant SCF Control(s):
- NET-14.5

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Secure telecommuting practices are defined.
(2) Technical measures govern remote access to systems and data for remote workers.
(3) Administrative measures govern rules of behavior for telecommuting practices.

11.21.11 Endpoint Security Validation

The entity must validate the security posture of the endpoint devices (e.g., software versions, patch levels, etc.) prior to allowing devices to connect to the entity's Technology Assets, Applications and/or Services (TAAS).

Relevant SCF Control(s):
- NET-14.7

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Cybersecurity / data privacy compliance checks are performed on constituent system components prior to the establishment of the internal connection.

11.21.12 Wireless Networking

The entity must control authorized wireless usage and monitor for unauthorized wireless access.

Relevant SCF Control(s):
- NET-15

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Usage restrictions are established for each type of wireless access to the system.

(2) *Connection requirements are established for each type of wireless access to the system.*
(3) *Wireless access points are identified.*

11.21.13 DNS & Content Filtering

The entity must force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.

Relevant SCF Control(s):
- NET-18

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Internet-bound network traffic is routed through a proxy device or service for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.*

11.22 Physical & Environmental Security

The entity must minimize physical access to the entity'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.

Relevant SCF Control(s):
- PES-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *The physical facility where the entity's systems reside is protected.*
(2) *The location or site of the facility where the system resides is planned considering physical and environmental hazards.*
(3) *For existing facilities, physical and environmental hazards are considered in the entity's risk management strategy.*
(4) *Physical security operations are conducted according to documented policies, standards, procedures and/or other entity directives.*
(5) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support physical security operations.*
(6) *Responsibility and authority for the performance of physical security-related activities are assigned to designated personnel.*

11.22.1 Physical Security Plan (PSP)

The entity must document a Physical Security Plan (PSP), or similar document, to summarize the implemented security controls to protect physical access to technology assets, as well as applicable risks and threats.

Relevant SCF Control(s):
- PES-01.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *A Site Security Plan (SitePlan) is documented 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.*

11.22.2 Zone-Based Physical Security

The entity must implement a zone-based approach to physical security.

Relevant SCF Control(s):
- PES-01.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A zone-based approach to physical security is:
   a. Developed; and
   b. Implemented.

11.22.3 Physical Access Authorizations

The entity must maintain a current list of personnel with authorized access to the entity's facilities (except for those areas within the facility officially designated as publicly accessible).

Relevant SCF Control(s):
- PES-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Authorized individuals allowed physical access are identified.
(2) Physical access to operating environments is limited to authorized individuals.
(3) Physical access to the entity's systems is limited to authorized individuals.
(4) Physical access to equipment is limited to authorized individuals.

11.22.4 Role-Based Physical Access

The entity must authorize physical access to facilities based on the position or role of the individual.

Relevant SCF Control(s):
- PES-02.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Physical access restrictions associated with changes to the system are defined and documented.
(2) The frequency at which to review the access list detailing authorized facility access by individuals is defined.

11.22.5 Physical Access Control

The entity must 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).

Relevant SCF Control(s):
- PES-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Physical access controls to control access to areas within the facility designated as publicly accessible are defined.
(2) Physical access authorizations are enforced at entry and exit points to the facility where the system resides by controlling ingress and egress with physical access control systems, devices, or guards.
(3) Physical access devices are:
   a. Identified; and
   b. Controlled.
(4) Visitors are escorted.

11.22.6 Physical Security of Offices, Rooms & Facilities

The entity must 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.

Relevant SCF Control(s):
- PES-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Physical security personnel inspect individuals 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.

11.22.7 Monitoring Physical Access

The entity must monitor for, detect and respond to physical security incidents.

Relevant SCF Control(s):

- PES-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The frequency at which to review physical access logs is defined.

(2) Events or potential indications of events requiring physical access logs to be reviewed are defined.

(3) Physical access to the facility where the system resides is monitored to detect physical security incidents.

(4) Physical access logs are reviewed per an entity-defined frequency.

11.22.8 Visitor Control

The entity must use physical access control mechanisms to identify, authorize and monitor visitors before allowing access to the facility (other than areas designated as publicly accessible).

Relevant SCF Control(s):

- PES-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Visitors are escorted.

(2) Visitor activity is controlled.

11.22.9 Equipment Siting & Protection

The entity must locate system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Relevant SCF Control(s):

- PES-12

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The location or site of the facility where the system resides is planned considering physical and environmental hazards.

(2) For existing facilities, physical and environmental hazards are considered in the entity's risk management strategy.

(3) Physical and environmental hazards that could result in potential damage to system components within the facility are defined.

(4) System components are positioned within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

11.23 Data Privacy

The entity must align data privacy engineering decisions with the entity's overall data privacy strategy and industry-recognized leading practices to secure Personal Data (PD) that implements the concept of data privacy by design and by default.

Relevant SCF Control(s):

- PRI-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An entity-wide privacy program plan that provides an overview of the agency's privacy program is developed.
(2) Data privacy operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(3) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support data privacy operations.
(4) Responsibility and authority for the performance of data privacy-related activities are assigned to designated personnel.

11.23.1 Reasonable Data Privacy Practices

The entity must limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD) according to reasonable consumer expectations for what is necessary and proportionate.

Relevant SCF Control(s):
- PRI-01.11

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Reasonable consumer expectations are defined for what is necessary and proportionate for collecting, receiving, processing, storage, transmission, sharing, updating and/or disposal of Personal Data (PD).
(2) Entity-specific practices are defined to limit the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of PD according to reasonable consumer expectations for what is necessary and proportionate.
(3) The collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of PD is limited to reasonable consumer expectations for what is necessary and proportionate.

11.23.2 Data Privacy Notice

The entity must:

(1) Make data privacy notice(s) available to individuals upon first interacting with an entity and subsequently as necessary;
(2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed;
(3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations;
(4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice;
(5) Periodically, review and update the content of the privacy notice, as necessary; and
(6) Retain prior versions of the privacy notice, in accordance with data retention requirements.

Relevant SCF Control(s):
- PRI-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Privacy notice(s) are developed and posted on all:*
    a. *External-facing websites;*
    b. *Mobile applications; and*
    c. *Other digital services.*
(2) The privacy notice(s) are written in plain language.
(3) The privacy notice(s) are organized in a way that is easy to understand and navigate.
(4) The privacy notice(s) provide the information needed by the public to make an informed decision about:
    a. Whether to interact with the entity.
    b. How to interact with the entity.
(5) The privacy notice(s) are updated whenever the entity makes a substantive change to the practices it describes.
(6) *The privacy notice(s) include a time/date stamp to inform the public of the date of the most recent changes.*

11.23.3 CHOICE & CONSENT

The entity must enable data subjects to authorize the collection, receiving, processing, storage, transmission, sharing, updating and/or disposal of their Personal Data (PD), where prior to collection the data subject is provided with:

(1) Plain language to illustrate the potential data privacy risks of the authorization;
(2) A means for users to decline the authorization; and
(3) All necessary choice and consent-related criteria required by applicable statutory, regulatory and contractual obligations.

Relevant SCF Control(s):

- PRI-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The tools or mechanisms to be implemented for individuals to consent to the processing of their Personal Data (PD) are defined.
(2) Tools or mechanisms are implemented for individuals to consent to the processing of their PD prior to its collection that facilitates individuals' informed decision-making.

11.23.4 RESTRICT COLLECTION TO IDENTIFIED PURPOSE

The entity must minimize the collection of Personal Data (PD) to only what is adequate, relevant and limited to the purposes identified in the data privacy notice, including protections against collecting PD from minors without appropriate parental or legal guardian consent.

Relevant SCF Control(s):

- PRI-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The type of processing of Personal Data (PD):
a. is defined; and
b. To be restricted is defined.

11.23.5 INVENTORY OF PERSONAL DATA (PD)

The entity must establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, share, update and/or dispose Personal Data (PD).

Relevant SCF Control(s):

- PRI-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Techniques used to dispose of information following the retention period are defined.
(2) Techniques used to destroy information following the retention period are defined.
(3) Techniques used to erase information following the retention period are defined.
(4) Organization-defined techniques are used to:
a. Dispose of information following the retention period.
b. Destroy information following the retention period.
c. Erase information following the retention period.

11.23.6 DATA SUBJECT EMPOWERMENT

The entity must provide authenticated data subjects the ability to:

(1) Access their Personal Data (PD) that is being processed, stored and shared, except where the burden, risk or expense of providing access would be disproportionate to the benefit offered to the data subject through granting access;
(2) Obtain answers on the specifics of how their PD is collected, received, processed, stored, transmitted, shared, updated and/or disposed;

(3) Obtain the source(s) of their PD;
(4) Obtain the categories of their PD being collected, received, processed, stored and shared;
(5) Request correction to their PD due to inaccuracies;
(6) Request erasure of their PD; and
(7) Restrict the further collecting, receiving, processing, storing, transmitting, updated and/or sharing of their PD.

Relevant SCF Control(s):
- PRI-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Mechanisms enabling individuals to have access to elements of their Personal Data (PD) are defined.
(2) Elements of PD to which individuals have access are defined.
(3) Entity-defined mechanisms are provided to enable individuals to have access to entity-defined elements of their PD.

11.23.7 Documenting Data Processing Activities

The entity must document Personal Data (PD) processing activities that covers collection, receiving, processing, storage, transmission, sharing, updating and/or disposal actions with sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual requirements.

Relevant SCF Control(s):
- PRI-14

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Privacy reports are defined.
(2) Privacy oversight bodies are defined.
(3) Officials responsible for monitoring privacy program compliance are defined.
(4) The frequency for reviewing and updating privacy reports is defined.
(5) Privacy reports are:
    a. Developed;
    b. Disseminated to oversight bodies to demonstrate accountability with statutory, regulatory and policy privacy mandates;
    c. Disseminated to officials; and
    d. Disseminated to other personnel responsible for monitoring privacy program compliance.
(6) Privacy reports are reviewed / updated frequently.

11.23.8 Data Subject Communications

The entity must craft disclosures and communications to data subjects in a manner that is concise, unambiguous and understandable by a reasonable person.

Relevant SCF Control(s):
- PRI-17

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Disclosures and communications to data subjects are:
    a. Made easily accessible; and
    b. Written in a manner that is concise, unambiguous and understandable by a reasonable person.

11.24 Project & Resource Management

The entity must ensure that security-related projects have both resource and project/program management support to ensure successful project execution.

Relevant SCF Control(s):
- PRM-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An entity-defined official is designated to manage the development, documentation and dissemination of the planning policy and procedures.
(2) Planning procedures facilitate the implementation of the planning policy and associated planning controls are developed and documented.
(3) Project & Resource Management (PRM) operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(4) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support PRM operations.
(5) Responsibility and authority for the performance of PRM-related activities are assigned to designated personnel.

11.24.1 Strategic Plan & Objectives

The entity must establish a:

(1) Strategic cybersecurity and data protection-specific business plan; and
(2) Set of objectives to achieve that plan.

Relevant SCF Control(s):
- PRM-01.1: Strategic Plan & Objectives

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A documented strategic cybersecurity and data protection-specific business plan exists.
(2) A documented set of objectives to achieve that cybersecurity and privacy-specific business plan exists.

11.24.2 Targeted Capability Maturity Levels

The entity must define and identify targeted capability maturity levels.

Relevant SCF Control(s):
- PRM-01.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The entity defines a Capability Maturity Model (CMM) it will use to benchmark maturity.
(2) Targeted capability maturity levels are defined at the domain and/or control level.

11.24.3 Allocation of Resources

The entity must identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects/initiatives.

Relevant SCF Control(s):
- PRM-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) High-level cybersecurity and data protection requirements for the system or system service are determined in mission and business process planning.
(2) The resources required to protect the system or system service are determined and documented as part of the entity's capital planning and investment control process.
(3) The resources required to protect the system or system service are allocated as part of the entity's capital planning and investment control process.
(4) A discrete line item for is established in the entity's programming and budgeting documentation.

11.24.4 Cybersecurity & Data Protection In Project Management

The entity must assess cybersecurity and data protection 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.

Relevant SCF Control(s):

- PRM-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Controls are assessed in the system and its environment of operation per an entity-defined 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 cybersecurity / data privacy requirements.*
(2) An appropriate assessor or assessment team is selected for the type of assessment to be conducted.
(3) A control assessment report is produced that documents the results of the assessment.
(4) *The results of the control assessment are provided to individuals or roles.*

11.24.5 Cybersecurity & Data Protection Requirements Definition

The entity must identify critical system components and functions by performing a criticality analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).

Relevant SCF Control(s):

- PRM-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Systems, system components or system services to be analyzed for criticality are defined.
(2) Decision points in the system development life cycle when a criticality analysis is to be performed are defined.
(3) Critical system components and functions are identified by performing a criticality analysis for systems, system components or system services at decision points in the system development life cycle.

11.24.6 Secure Development Life Cycle (SDLC) Management

The entity must ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.

Relevant SCF Control(s):

- PRM-07

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) System development life cycle is defined.
(2) The system is acquired, developed and managed using entity-defined System Development Lifecycle (SDLC) that incorporates information cybersecurity / data privacy considerations.
(3) Cybersecurity / data privacy roles and responsibilities are defined and documented throughout the SDLC.
(4) Individuals with cybersecurity / data privacy roles and responsibilities are identified.
(5) Entity cybersecurity / data privacy risk management processes are integrated into SDLC activities.

11.25 Risk Management

The entity must ensure that the business unit(s) that own the assets and / or processes involved are made aware of and understand all applicable cybersecurity and data protection-related risks. The cybersecurity and data protection teams advise and educate on risk management matters, while it is the business units and other key stakeholders that ultimately own the risk.

Relevant SCF Control(s):

- RSK-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A comprehensive strategy is developed to manage cybersecurity and data protection risk to the entity's operations and assets, individuals and other entities associated with the operation and use of the entity's systems.
(2) The risk management strategy is implemented consistently across the entity.
(3) A senior the entity's position for Risk Management aligns cybersecurity and data protection management processes with strategic, operational and budgetary planning processes.
(4) For existing facilities, physical and environmental hazards are considered in the entity's risk management strategy.
(5) Risk management operations are conducted according to documented policies, standards, procedures and/or other directives.
(6) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support risk management operations.
(7) Responsibility and authority for the performance of risk management-related activities are assigned to designated personnel.

11.25.1 Risk Framing

The entity must identify:

(1) Assumptions affecting risk assessments, risk response and risk monitoring;
(2) Constraints affecting risk assessments, risk response and risk monitoring;
(3) The the entity's risk tolerance; and
(4) Priorities, benefits and trade-offs considered by the entity for managing risk.

Relevant SCF Control(s):

- RSK-01.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A comprehensive strategy is developed to manage cybersecurity / data privacy risk to entity operations and assets, individuals and other entities associated with the operation and use of entity systems.
(2) The risk management strategy is implemented consistently across the entity.
(3) A senior entity position for risk management aligns cybersecurity / data privacy management processes with strategic, operational and budgetary planning processes.
(4) For existing facilities, physical and environmental hazards are considered in the the entity's risk management strategy.

11.25.2 Risk Tolerance

The entity must define its risk tolerance, the specified range of acceptable results.

Relevant SCF Control(s):

- RSK-01.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An executive steering committee, or advisory board, defines the entity's risk tolerance.

11.25.3 Risk Threshold

The entity must define its risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.

Relevant SCF Control(s):

- RSK-01.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An executive steering committee, or advisory board, defines the entity's risk threshold.

11.25.4 Risk Appetite

The entity must define its risk appetite, the degree of uncertainty it is willing to accept in anticipation of a reward.

Relevant SCF Control(s):

- RSK-01.5

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An executive steering committee, or advisory board, defines the entity's risk appetite.

11.25.5 Risk Identification

The entity must identify and documents risks, both internal and external.

Relevant SCF Control(s):

- RSK-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A process exists to identify applicable internal and external risks.

(2) Applicable internal and external risks are documented.

11.25.6 Risk Catalog

The entity must develop and keep current a catalog of applicable risks associated with its business operations and technologies in use.

Relevant SCF Control(s):

- RSK-03.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A risk catalog, or similar solution, exists that keeps current a catalog of applicable risks associated with the entity's business operations and technologies in use.

11.25.7 Risk Assessment

The entity must conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the entity's Technology Assets, Applications, Services and/or Data (TAASD).

Relevant SCF Control(s):

- RSK-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The frequency to assess risk to the entity's operations, the entity's assets and individuals is defined.

(2) A document in which risk assessment results are to be documented (if not documented in the cybersecurity and data protection plans or risk assessment report) is defined.

(3) A risk assessment is conducted to determine the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification or destruction of the system. the information it processes, stores or transmits. and any related information.

(4) Personnel or roles to whom risk assessment results are to be disseminated is/are defined.

(5) Risk assessment results are disseminated to personnel or roles.

(6) Risk assessments are updated per an entity-defined frequency.

11.25.8 Risk Register

The entity must maintain a risk register that facilitates monitoring and reporting of risks.

Relevant SCF Control(s):
- RSK-04.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A risk register is maintained to facilitate the monitoring and reporting of risks.

11.25.9 Risk Assessment Methodology

The entity must implement a risk assessment methodology to ensure coverage for its components relevant for secure, compliant and resilient operations.

Relevant SCF Control(s):
- RSK-04.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A risk assessment methodology that can cover the entity's components relevant for secure, compliant and resilient operations is defined.

(2) A risk assessment methodology that covers the entity's components relevant for secure, compliant and resilient operations is implemented.

11.25.10 Risk Ranking

The entity must identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.

Relevant SCF Control(s):
- RSK-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Newly discovered risks are ranked based on industry-recognized practices.

11.25.11 Risk Remediation

The entity must remediate risks to an acceptable level.

Relevant SCF Control(s):
- RSK-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A defined risk threshold exists to determine what risk is and is not acceptable.

(2) Data / process owners are held accountable to remediate risks to an acceptable level.

(3) The entity utilizes compensating controls to remediate control deficiencies to an acceptable level.

11.25.12 Risk Response

The entity must respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed.

Relevant SCF Control(s):
- RSK-06.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Findings from security assessments are responded to in accordance with the entity's risk tolerance.*

11.25.13 Compensating Countermeasures

The entity must identify and implement compensating countermeasures to reduce risk and exposure to threats.

Relevant SCF Control(s):

- RSK-06.2

NOTE: A material control is not eligible to have a compensating control, since a material control is such a fundamental cybersecurity and/or data protection control that:

- *It is not capable of having compensating controls; and*
- *Its absence, or failure, exposes an entity to such a degree that it could have a material impact.*

To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Identified and implemented compensating countermeasures to reduce risk and exposure to threats.*

11.25.14 Risk Treatment Plan

The entity must formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.

Relevant SCF Control(s):

- RSK-06.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *A Risk Treatment Plan (RTP) format is defined.*
(2) *A RTP is utilized for applicable stakeholders to remediate identified risks according to a defined timeline.*

11.25.15 Supply Chain Risk Management (SCRM) Plan

The entity must develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.

Relevant SCF Control(s):

- RSK-09

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *An entity-wide strategy for managing supply chain risks is developed.*
(2) *Supply chain risks associated with the entity's systems and system components are identified.*
(3) *The supply chain risk management strategy is implemented consistently across the entity.*
(4) *A plan for managing supply chain risks is developed.*
(5) *Security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events are defined.*
(6) *Per an entity-defined frequency, the SCRM plan is:*
    a. *Reviewed; and*
    b. *Updated.*

11.25.16 Supply Chain Risk Assessment

The entity must periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).

Relevant SCF Control(s):

- RSK-09.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Supply chain risks associated with the entity's systems and system components are:
- *a. Identified;*
- *b. Assessed; and*
- *c. Responded to.*

11.25.17 Data Protection Impact Assessment (DPIA)

The entity must conduct a Data Protection Impact Assessment (DPIA) on Technology Assets, Applications and/or Services (TAAS) that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.

Relevant SCF Control(s):
- RSK-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Data Protection Impact Assessments (DPIAs) are conducted for systems, programs or other activities before:
- *a. Developing or procuring information technology that processes Personal Data (PD);*
- *b. Initiating a collection of PD that will be processed using information technology; and/or*
- *c. Initiating a collection of PD that includes PD permitting the physical or virtual (online) contacting of a specific individual.*

11.26 Secure Engineering & Architecture

The entity must align cybersecurity engineering and architecture decisions with the entity's overall technology architectural strategy and industry-recognized leading practices to secure networked environments.

Relevant SCF Control(s):
- SEA-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Secure engineering principles are defined.
(2) Data privacy engineering principles are defined.
(3) Architectural designs that promote effective cybersecurity and data protection are identified.
(4) Systems engineering principles that promote effective cybersecurity and data protection are identified.
(5) Identified architectural designs that promote effective cybersecurity and data protection are employed.
(6) Identified systems engineering principles that promote effective cybersecurity and data protection are employed.
(7) Secure Engineering & Architecture (SEA) operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(8) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support SEA operations.
(9) Responsibility and authority for the performance of SEA-related activities are assigned to designated personnel.

11.26.1 Secure Engineering Principles

The entity must facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).

Relevant SCF Control(s):
- SEA-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Secure engineering principles are defined.*
(2) *Data privacy engineering principles are defined.*
(3) *Architectural designs that promote effective cybersecurity and data protection are identified.*
(4) *Systems engineering principles that promote effective cybersecurity and data protection are identified.*
(5) *Identified architectural designs that promote effective cybersecurity and data protection are employed.*
(6) *Identified systems engineering principles that promote effective cybersecurity and data protection are employed.*
(7) *Secure Engineering & Architecture (SEA) operations are conducted according to documented policies, standards, procedures and/or other entity directives.*
(8) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support SEA operations.*
(9) *Responsibility and authority for the performance of SEA-related activities are assigned to designated personnel.*

11.26.2 Achieving Resilience Requirements

The entity must achieve resilience requirements in normal and adverse situations.

Relevant SCF Control(s):
- SEA-01.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *The entity's goals for resiliency are defined for normal and adverse situations.*
(2) *Solutions exist to achieve resilience requirements in:*
    a. *Normal situations; and*
    b. *Adverse situations.*

11.26.3 Resilience Capabilities

The entity must ensure cybersecurity and data protection controls are designed and implemented to provide resistance to:
(1) Unintentional errors (by users or software); and
(2) Intentional attack or circumvention.

Relevant SCF Control(s):
- SEA-01.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Cybersecurity and data protection controls are designed and implemented to provide resistance to:*
    a. *Unintentional errors (by users or software); and*
    b. *Intentional attack or circumvention.*

11.26.4 Alignment With Enterprise Architecture

The entity must develop an enterprise architecture, aligned with industry-recognized secure practices, with consideration for cybersecurity and data protection principles that addresses risk to its operations, assets, individuals and other entities.

Relevant SCF Control(s):
- SEA-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *An enterprise architecture is developed with consideration for cybersecurity and data protection.*
(2) *An enterprise architecture is maintained with consideration for cybersecurity and data protection.*
(3) *An enterprise architecture is developed with consideration for the resulting risk to the entity's operations and assets, individuals and other entities.*
(4) *An enterprise architecture is maintained with consideration for the resulting risk to the entity's operations and assets, individuals and other entities.*

11.26.5 Technical Debt Reviews

The entity must conduct ongoing "technical debt" reviews of hardware and software technologies to remediate outdated and/or unsupported technologies.

Relevant SCF Control(s):
- SEA-02.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) "Technical debt" reviews of hardware and software technologies are routinely conducted.

(2) The results of "technical debt" reviews are leveraged as justification to remediate outdated and/or unsupported technologies.

11.26.6 Defense-In-Depth (DiD) Architecture

The entity must 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.

Relevant SCF Control(s):
- SEA-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Security functions are implemented 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.

(2) The cybersecurity and data protection architecture for the system is designed using a defense-in-depth approach that allocates controls to locations and architectural layers.

(3) The cybersecurity and data protection architecture for the system is designed using a defense-in-depth approach that ensures the allocated controls operate in a coordinated and mutually reinforcing manner.

11.26.7 Clock Synchronization

The entity must utilize time-synchronization technology to synchronize all critical system clocks.

Relevant SCF Control(s):
- SEA-20

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Internal system clocks are used to generate timestamps for audit records.

11.27 Security Operations

The entity must ensure appropriate resources and a management structure exists to enable the delivery of cybersecurity, physical security and data privacy operations.

Relevant SCF Control(s):
- OPS-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Operations security controls to be employed to protect key the entity's information throughout the system development life cycle are defined.

(2) Operations security controls are employed to protect key the entity's information throughout the system development life cycle.

(3) Security operations are conducted according to documented policies, standards, procedures and/or other entity directives.

(4) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support security operations.*
(5) *Responsibility and authority for the performance of security operations-related activities are assigned to designated personnel.*

11.27.1 Standardized Operating Procedures (SOP)

The entity must identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.

Relevant SCF Control(s):
- OPS-01.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Procedures needed to satisfy the security requirements for the protection of sensitive / regulated data are:*
    a. *Developed and documented.*
    b. *Disseminated to the entity's personnel or roles.*

11.27.2 Security Concept Of Operations (CONOPS)

The entity must 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.

Relevant SCF Control(s):
- OPS-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *A Concept of Operations (CONOPS) for the system describing how the entity intends to operate the system from the perspective of cybersecurity and data protection is developed.*

11.27.3 Service Delivery (Business Process Support)

The entity must define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the entity's technology capabilities supporting business functions, workforce and/or customers based on industry-recognized standards to achieve the specific goals of the process area.

Relevant SCF Control(s):
- OPS-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Supporting business processes are defined.*
(2) *Appropriate governance and service management is implemented to ensure appropriate planning, delivery and support of business functions, workforce and/or customers.*

11.28 Security Awareness & Training

The entity must develop a cybersecurity and data protection-minded workforce through continuous education activities and practical exercises.

Relevant SCF Control(s):
- SAT-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A cybersecurity and data protection workforce development and improvement program is established.
(2) The cybersecurity and data protection education and awareness program is entity-wide.
(3) Security literacy training is provided to system users per an entity-defined frequency after initial training.
(4) Security Awareness & Training (SAT) operations are conducted according to documented policies, standards and procedures.
(5) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support SAT operations.
(6) Responsibility and authority for the performance of SAT-related activities are assigned to designated personnel.

11.28.1 Cybersecurity & Data Protection-Minded Workforce

The entity must provide all employees and contractors with appropriate awareness education and training that is relevant for their job function.

Relevant SCF Control(s):

- SAT-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A cybersecurity and data protection workforce development and improvement program is established.
(2) The cybersecurity and data protection education and awareness program is entity-wide.
(3) Security literacy training is provided to system users per an entity-defined frequency after initial training.
(4) Security Awareness & Training (SAT) operations are conducted according to documented policies, standards and procedures.
(5) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support SAT operations.
(6) Responsibility and authority for the performance of SAT-related activities are assigned to designated personnel.

11.28.2 Cybersecurity & Data Protection Awareness Training

The entity must provide all employees and contractors with appropriate awareness education and training that is relevant for their job function.

Relevant SCF Control(s):

- SAT-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Cybersecurity and data protection literacy training is provided to system users (including managers, senior executives and contractors) as part of initial training for new users.
(2) Cybersecurity and data protection literacy training is provided to system users (including managers, senior executives and contractors) entity-defined frequency thereafter.

11.28.3 Role-Based Cybersecurity & Data Protection Training

The entity must provide role-based cybersecurity and data protection-related training:

(1) Before authorizing access to the system or performing assigned duties;
(2) When required by system changes; and
(3) Annually thereafter.

Relevant SCF Control(s):

- SAT-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Roles and responsibilities for role-based cybersecurity and data protection training are defined.
(2) Events that require role-based security training content updates are defined.
(3) Role-based cybersecurity and data protection training is provided to the entity's personnel:
    a. Before authorizing access to the system or sensitive and/or regulated data;
    b. Before performing assigned duties; and
    c. Per an entity-defined frequency after initial training.
(4) Role-based cybersecurity and data protection training is provided to the entity's personnel when required by system changes or following entity-defined events.

11.29 Technology Development & Acquisition

The entity must ensure that cybersecurity and data protection 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.

Relevant SCF Control(s):

- TDA-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A system and services acquisition policy is developed and documented.
(2) System and services acquisition procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls are developed and documented.
(3) Acquisition strategies, contract tools and procurement methods are implemented to:
    a. Identify supply chain risks;
    b. Protect against supply chain risks; and
    c. Mitigate supply chain risks.
(4) Technology Development & Acquisition (TDA) operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(5) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support TDA operations.
(6) Responsibility and authority for the performance of TDA-related activities are assigned to designated personnel.

11.29.1 Technology Development & Acquisition

The entity must facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.

Relevant SCF Control(s):

- TDA-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A system and services acquisition policy is developed and documented.
(2) System and services acquisition procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls are developed and documented.

(3) *Acquisition strategies, contract tools and procurement methods are implemented to:*
   a. *Identify supply chain risks;*
   b. *Protect against supply chain risks; and*
   c. *Mitigate supply chain risks.*
(4) *Technology Development & Acquisition (TDA) operations are conducted according to documented policies, standards, procedures and/or other entity directives.*
(5) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support TDA operations.*
(6) *Responsibility and authority for the performance of TDA-related activities are assigned to designated personnel.*

11.29.2 Product Management

The entity must design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:
(1) Improve functionality;
(2) Enhance security and resiliency capabilities;
(3) Correct security deficiencies; and
(4) Conform with applicable statutory, regulatory and/or contractual obligations.

Relevant SCF Control(s):
- TDA-01.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Product management processes are designed and implemented to ensure products, including systems, software and services, are routinely updated to improve functionality and correct security deficiencies.
(2) Systems or system components supporting mission-essential services or functions are defined.
(3) Entity-defined criteria are employed on systems or system components supporting essential services or functions to increase the trustworthiness in those systems or components.

11.29.3 DevSecOps

The entity must integrate cybersecurity and data protection into Development, Security and Operations (DevSecOps) to prioritize secure practices throughout the Software Development Lifecycle (SDLC).

Relevant SCF Control(s):
- TDA-01.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Cybersecurity / data privacy is integrated into emerging Development and Operations (DevOps) to prioritize secure practices throughout the Software Development Lifecycle (SDLC).

11.29.4 Minimum Viable Product (MVP) Security Requirements

The entity must design, develop and produce Technology Assets, Applications and/or Services (TAAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.

Relevant SCF Control(s):
- TDA-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Cybersecurity / data privacy functional requirements, descriptions and criteria are included explicitly or by reference using in the acquisition contract for the system, system component or system service.
(2) Strength of mechanism requirements, descriptions and criteria are included explicitly or by reference using in the acquisition contract for the system, system component or system service.

(3) *Cybersecurity / data privacy assurance requirements, descriptions and criteria are included explicitly or by reference using in the acquisition contract for the system, system component or system service.*
(4) *Controls needed to satisfy the cybersecurity / data requirements, descriptions and criteria are included explicitly or by reference using in the acquisition contract for the system, system component or system service.*

11.29.5 Development Methods, Techniques & Processes

The entity must require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.

Relevant SCF Control(s):
- TDA-02.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) Cybersecurity / data privacy systems engineering methods are defined.
(2) Software development methods are defined.
(3) Testing, evaluation, assessment, verification and validation methods are defined.
(4) Quality control processes are defined.
(5) The developer of the system, system component or system service is required to demonstrate the use of a system development life cycle process that includes entity-defined system security engineering methods.

11.29.6 Product Testing & Reviews

The entity must regularly review Technology Assets, Applications and/or Services (TAAS) for an appropriate level of security and resiliency based on applicable risks and threats.

Relevant SCF Control(s):
- TDA-02.10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) An appropriate level of security and resiliency for products and/or services is defined.
(2) Products and/or services are regularly reviewed for an appropriate level of security and resiliency based on applicable risks and threats.

11.29.7 Software Bill of Materials (SBOM)

The entity must generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.

Relevant SCF Control(s):
- TDA-04.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *A SBOM for systems, applications and services lists software packages in use, including versions and applicable licenses.*

11.29.8 Developer Architecture & Design

The entity must require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that:
(1) Is consistent with and supportive of the entity's security architecture which is established within and is an integrated part of the entity's enterprise architecture;
(2) Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and

(3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.

Relevant SCF Control(s):
- TDA-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The developer of the system, system component or system service is required to produce a design specification and cybersecurity / data privacy architecture that:
- *a. Are consistent with the entity's security architecture, which is an integral part the entity's enterprise architecture;*
- *b. Accurately and completely describe the required security functionality and the allocation of controls among physical and logical components; and*
- *c. Express how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.*

11.29.9 Secure Software Development Practices (SSDP)

The entity must develop applications based on Secure Software Development Practices (SSDP).

Relevant SCF Control(s):
- TDA-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Software development techniques that promote effective cybersecurity and data protection are identified.
(2) Testing, evaluation, assessment, verification and validation methods are defined.
(3) Cybersecurity and data protection requirements to be satisfied by the process, standards, tools, tool options and tool configurations are defined.
(4) Identified software development techniques that promote effective cybersecurity and data protection are employed.

11.29.10 Criticality Analysis

The entity must develop applications based on Secure Software Development Practices (SSDP).

Relevant SCF Control(s):
- TDA-06.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Decision points in the system development life cycle are defined.
(2) The breadth of criticality analysis is defined.
(3) The depth of criticality analysis is defined.
(4) The developer of the system, system component, or system service is required to perform a criticality analysis:
- *a. At entity-defined decision points in the system development life cycle;*
- *b. Per an entity-defined breadth; and*
- *c. Per an entity-defined depth.*

(5) Suppliers of critical or mission-essential technologies, products and services are:
- *a. Identified;*
- *b. Prioritized; and*
- *c. Assessed.*

11.29.11 Threat Modeling

The entity must perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.

Relevant SCF Control(s):
- TDA-06.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A supporting toolchain helps ensure the accuracy, consistency and comprehensiveness of secure practices throughout the asset's lifecycle.

11.29.12 Software Design Review

The entity must have an independent review of the software design to confirm that all cybersecurity and data protection requirements are met and that any identified risks are satisfactorily addressed.

Relevant SCF Control(s):
- TDA-06.5

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An independent review of the software design confirms that all cybersecurity / data privacy requirements are met and that any identified risks are satisfactorily addressed.

11.29.13 Secure Development Environments

The entity must maintain a segmented development network to ensure a secure development environment.

Relevant SCF Control(s):
- TDA-07

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) System pre-production environments are protected commensurate with risk throughout the system development life cycle for the system, system component or system service.

11.29.14 Access to Program Source Code

The entity must limit privileges to change software resident within software libraries.

Relevant SCF Control(s):
- TDA-20

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Entity-defined criteria for security-relevant information pertaining to external system interfaces, high-level design, low-level design, source code or hardware schematics and design and implementation information are documented in a System Security Plan (SSP).

(2) The developer of the system, system component or system service is required to provide design and implementation information for the controls that includes using at level of detail.

11.30 Third-Party Management

The entity must ensure that cybersecurity and data protection risks associated with third-parties are minimized and enable measures to sustain operations should a third-party become compromised, untrustworthy or defunct.

Relevant SCF Control(s):
- TPM-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Security requirements to protect against supply chain risks to the system, system components, or system services and to limit the harm or consequences from supply chain-related events are defined.*
(2) *Cybersecurity and data protection functional requirements, descriptions and criteria are included explicitly or by reference using in the acquisition contract for the system, system component or system service.*
(3) *Requirements for protecting cybersecurity and data protection documentation, descriptions and criteria are included explicitly or by reference using in the acquisition contract for the system, system component or system service.*
(4) *Strength of mechanism requirements, descriptions and criteria are included explicitly or by reference using in the acquisition contract for the system, system component or system service.*
(5) *Cybersecurity and data protection assurance requirements, descriptions and criteria are included explicitly or by reference using in the acquisition contract for the system, system component or system service.*
(6) *Controls needed to satisfy the cybersecurity and data protection requirements, descriptions and criteria are included explicitly or by reference using in the acquisition contract for the system, system component or system service.*
(7) *Third-party management operations are conducted according to documented policies, standards, procedures and/or other entity directives.*
(8) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support third-party management operations.*
(9) *Responsibility and authority for the performance of third-party management-related activities are assigned to designated personnel.*

11.30.1 Third-Party Inventories

The entity must maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the entity must's Technology Assets, Applications, Services and/or Data (TAASD).

Relevant SCF Control(s):
- TPM-01.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *A current, accurate and complete list of ESPs that can potentially impact the Sensitivity, Integrity, Availability and/or Safety (CIAS) of the entity's systems, applications, services and data is maintained.*

11.30.2 Third-Party Criticality Assessments

The entity must identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.

Relevant SCF Control(s):
- TPM-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Systems, system components or system services to be analyzed for criticality are defined.*
(2) *Decision points in the system development life cycle when a criticality analysis is to be performed are defined.*
(3) *Critical system components and functions are identified by performing a criticality analysis for systems, system components or system services at decision points in the system development life cycle.*
(4) *Suppliers of critical or mission-essential technologies, products and services are:*
    a. *Identified;*
    b. *Prioritized; and*
    c. *Assessed.*

11.30.3 Supply Chain Risk Management (SCRM)

The entity must:
(1) Evaluate security risks and threats associated with the Technology Assets, Applications and/or Services (TAAS) supply chains; and

(2) Take appropriate remediation actions to minimize the entity must's exposure to those risks and threats, as necessary.

Relevant SCF Control(s):
- TPM-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The personnel, roles and responsibilities of the supply chain risk management team are defined.
(2) Supply chain risk management activities are defined.
(3) A supply chain risk management team consisting of personnel, roles and responsibilities is established to lead and support supply chain risk management activities.
(4) The supply chain risk management plan addresses risks associated with the:
  a. Research and development of systems, system components or system services;
  b. Design of systems, system components or system services;
  c. Manufacturing of systems, system components or system services;
  d. Acquisition of systems, system components or system services;
  e. Delivery of systems, system components or system services;
  f. Integration of systems, system components or system services;
  g. Operation and maintenance of systems, system components or system services; and
  h. Disposal of systems, system components or system services.

11.30.4 Third-Party Services

The entity must mitigate the risks associated with third-party access to the entity's Technology Assets, Applications, Services and/or Data (TAASD).

Relevant SCF Control(s):
- TPM-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Controls to be employed by external system service providers are defined.
(2) Processes, methods and techniques employed to monitor control compliance by external service providers are defined.
(3) Providers of external system services comply with the entity's cybersecurity / data privacy requirements.
(4) Providers of external system services employ controls.

11.30.5 Third-Party Risk Assessments & Approvals

The entity must conduct a risk assessment prior to the acquisition or outsourcing of technology-related TAAS.

Relevant SCF Control(s):
- TPM-04.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Personnel or roles that approve the acquisition or outsourcing of dedicated cybersecurity services is/are defined.
(2) An the entity's assessment of risk is conducted prior to the acquisition or outsourcing of cybersecurity services.
(3) Personnel or roles approve the acquisition or outsourcing of dedicated cybersecurity services.

11.30.6 Third-Party Processing, Storage and Service Locations

The entity must restrict the location of information processing/storage based on business requirements.

Relevant SCF Control(s):
- TPM-04.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Locations where information processing and data storage is/are to be restricted are defined.
(2) Requirements or conditions for restricting the location of information processing, information storage or information services are defined.
(3) Based on requirements, information processing, information storage or information services is/are restricted to locations.
(4) The location or site of the facility where the system resides is planned considering physical and environmental hazards.
(5) For existing facilities, physical and environmental hazards are considered in the the entity's risk management strategy.

11.30.7 Third-Party Contract Requirements

The entity must require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the entity must's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).

Relevant SCF Control(s):
- TPM-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Legally-binding contracts are executed to enforce cybersecurity and data protection requirements by third-parties.
(2) Before sharing sensitive and/or regulated data, Non-Disclosure Agreements (NDAs) are executed with third parties.
(3) Security requirements to be satisfied by external system service providers are defined.
(4) The providers of external system services used for the processing, storage, or transmission of sensitive and/or regulated data comply with entity-defined security requirements.

11.30.8 Contract Flow-Down Requirements

The entity must ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.

Relevant SCF Control(s):
- TPM-05.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The controls included in the contracts of prime contractors are also included in the contracts of subcontractors.
(2) Security requirements to be satisfied by external system service providers are defined.

11.30.9 Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix

The entity must document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).

Relevant SCF Control(s):
- TPM-05.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, delineates assignment for cybersecurity and data protection controls between internal stakeholders and ESP.
(2) User roles and responsibilities with regard to external system services, including shared responsibilities with external service providers, are defined and documented.

11.30.10 Break Clauses

The entity must include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data protection controls.

Relevant SCF Control(s):
- TPM-05.7

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Contracts with third-parties include "break clauses" to enable the entity to exit a contract due to a third-party's non-compliance with contract requirements for cybersecurity / data privacy controls.

11.31 THREAT MANAGEMENT

The entity must establish a capability to proactively identify and manage technology-related threats to the cybersecurity and data protection of the entity's systems, data and business processes.

Relevant SCF Control(s):
- THR-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A threat awareness program that includes a cross-entity information-sharing capability for threat intelligence is implemented.
(2) Sources of threat intelligence are defined.
(3) A risk assessment methodology is identified.
(4) Sources of threat intelligence are employed as part of a risk assessment to guide and inform:
  a. The development of the entity's systems and security architectures;
  b. The selection of security solutions;
  c. System monitoring activities;
  d. Threat hunting activities; and
  e. Response and recovery activities.
(5) Threat management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(6) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support threat management operations.
(7) Responsibility and authority for the performance of threat management-related activities are assigned to designated personnel.

11.31.1 THREAT INTELLIGENCE PROGRAM

The entity must implement a threat intelligence program that includes a cross-entity 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.

Relevant SCF Control(s):
- THR-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A threat awareness program that includes a cross-entity information-sharing capability for threat intelligence is implemented.
(2) Sources of threat intelligence are defined.
(3) A risk assessment methodology is identified.
(4) Sources of threat intelligence are employed as part of a risk assessment to guide and inform:
  a. The development of the entity's systems and security architectures;
  b. The selection of security solutions;
  c. System monitoring activities;
  d. Threat hunting activities; and

e. *Response and recovery activities.*

(5) *Threat management operations are conducted according to documented policies, standards, procedures and/or other entity directives.*

(6) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support threat management operations.*

(7) *Responsibility and authority for the performance of threat management-related activities are assigned to designated personnel.*

11.31.2 Threat Intelligence Feeds

The entity must maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.

Relevant SCF Control(s):

- THR-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *External entities from whom system security alerts, advisories and directives are to be received on an ongoing basis are defined.*

(2) *Personnel or roles to whom security alerts, advisories and directives are to be disseminated is/are defined.*

(3) *Elements within the entity to whom security alerts, advisories and directives are to be disseminated are defined.*

(4) *External entities to whom security alerts, advisories and directives are to be disseminated are defined.*

(5) *System security alerts, advisories and directives from external entities are received on an ongoing basis.*

(6) *Threat indicator information is identified.*

(7) *Effective mitigations are identified.*

(8) *Intrusion detection approaches are identified.*

(9) *Threat hunting activities are identified.*

11.31.3 Threat Intelligence Reporting

The entity must utilize external threat intelligence feeds to generate and disseminate entity-specific security alerts, advisories and/or directives.

Relevant SCF Control(s):

- THR-03.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Internal security alerts, advisories and directives are generated, as necessary.*

(2) *Internal security alerts, advisories and directives are disseminated, as necessary.*

11.31.4 Threat Catalog

The entity must develop and maintain current a catalog of applicable internal and external threats to the entity, both natural and manmade.

Relevant SCF Control(s):

- THR-09

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *The entity maintains a threat catalog that documents applicable internal and external threats that are specific to the entity.*

(2) *The threat catalog documents both natural and manmade threats.*

(3) *On at least an annual basis, a threat assessment is performed to identify and assess applicable internal and external threats.*

(4) *The threat catalog is updated, based on a current threat assessment.*

11.31.5 THREAT ANALYSIS

The entity must identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.

Relevant SCF Control(s):

- THR-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) On at least an annual basis, a threat assessment is performed to identify and assess applicable internal and external threats.
(2) A threat catalog captures applicable internal and external threats from the threat assessment.
(3) Each item in the threat catalog is prioritized, based on the potential threat to the entity.

11.32 VULNERABILITY & PATCH MANAGEMENT

The entity must proactively manage the risks associated with technical vulnerability management that includes ensuring good patch and change management practices are utilized.

Relevant SCF Control(s):

- VPM-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An entity-wide vulnerability and patch management program is developed and implemented to proactively identify and remediation vulnerabilities.
(2) For system flaws, the time is specified in which to:
    a. Identify;
    b. Report; and
    c. Correct.
(3) Within the entity-specified time frame, system flaws are:
    a. Identified;
    b. Reported; and
    c. Corrected.
(4) Vulnerability & patch management operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(5) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support vulnerability & patch management operations.
(6) Responsibility and authority for the performance of vulnerability & patch management-related activities are assigned to designated personnel.

11.32.1 VULNERABILITY & PATCH MANAGEMENT PROGRAM (VPMP)

The entity must ensure that vulnerabilities are properly identified, tracked and remediated.

Relevant SCF Control(s):

- VPM-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An entity-wide vulnerability and patch management program is developed and implemented to proactively identify and remediation vulnerabilities.
(2) For system flaws, the time is specified in which to:
    a. Identify;
    b. Report; and

c. *Correct.*

(3) *Within the entity-specified time frame, system flaws are:*
   a. *Identified;*
   b. *Reported; and*
   c. *Corrected.*

(4) *Vulnerability & patch management operations are conducted according to documented policies, standards, procedures and/or other entity directives.*

(5) *Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support vulnerability & patch management operations.*

(6) *Responsibility and authority for the performance of vulnerability & patch management-related activities are assigned to designated personnel.*

11.32.2 Vulnerability Remediation Process

The entity must ensure that vulnerabilities are properly identified, tracked and remediated.

Relevant SCF Control(s):
- VPM-02

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Vulnerabilities are identified.*

(2) *Response times to remediate system vulnerabilities are defined.*

(3) *Vulnerabilities are remediated in accordance with risk assessments.*

11.32.3 Vulnerability Ranking

The entity must ensure that vulnerabilities are properly identified, tracked and remediated.

Relevant SCF Control(s):
- VPM-03

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *A risk ranking methodology is utilized to prioritize newly discovered security vulnerabilities.*

11.32.4 Software & Firmware Patching

The entity must conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.

Relevant SCF Control(s):
- VPM-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *The time period within which to install security-relevant software updates after the release of the updates is defined.*

(2) *System flaws are identified.*

(3) *Automated patch management tools are employed to facilitate flaw remediation to components.*

(4) *System flaws are corrected.*

(5) *System vulnerabilities are remediated within entity-defined response times.*

(6) *Security-relevant software updates are installed within an entity-defined time period of the release of the updates.*

(7) *Security-relevant firmware updates are installed within an entity-defined time of the release of the updates.*

11.32.5 Vulnerability Scanning

The entity must detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.

Relevant SCF Control(s):

- VPM-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The frequency at which the system is scanned for vulnerabilities is defined.
(2) Response times to remediate legitimate vulnerabilities in accordance with the entity's assessment of risk are defined.
(3) Personnel or roles with whom information obtained from the vulnerability scanning process and control assessments are to be shared.
(4) Vulnerability scan reports and results from vulnerability monitoring are analyzed.
(5) Systems and hosted applications are scanned for vulnerabilities frequently and/or randomly in accordance with entity-defined process and when new vulnerabilities potentially affecting the system are identified and reported.

11.32.6 Breadth / Depth of Coverage

The entity must identify the breadth and depth of coverage for vulnerability scanning that define the system components scanned and types of vulnerabilities that are checked for.

Relevant SCF Control(s):

- VPM-06.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The breadth and depth of vulnerability scanning coverage are defined.

11.33 Web Security

The entity must address the risks associated with Internet-accessible technologies by hardening devices, monitoring system file integrity, enabling auditing and monitoring for malicious activities.

Relevant SCF Control(s):

- WEB-01

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) An enterprise-wide web management policy, as well as associated standards, controls and procedures exists.
(2) Web security operations are conducted according to documented policies, standards, procedures and/or other entity directives.
(3) Adequate resources (e.g., people, processes, technologies, data and/or facilities) are provided to support web security operations.
(4) Responsibility and authority for the performance of web security-related activities are assigned to designated personnel.

11.33.1 Strong Customer Authentication (SCA)

The entity must implement Strong Customer Authentication (SCA) for consumers to reasonably prove their identity.

Relevant SCF Control(s):

- WEB-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Strong Customer Authentication (SCA) is utilized for consumers and/or data subjects to prove their identity.

11.33.2 Secure Web Traffic

The entity must ensure all web application content is delivered using cryptographic mechanisms (e.g., TLS).

Relevant SCF Control(s):

- WEB-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) All web application content is delivered using cryptographic mechanisms.

12 Due Care Activities

As described in Section 7 – Control Set Determination, the Minimum Security Requirements (MSR) is a baseline determined by the entity's Minimum Compliance Requirements (MCR) and Discretionary Security Requirements (DSR). While compliance-related activities are unique to the statutory, regulatory or contractual obligations of the entity, there are reasonable cybersecurity and data protection capabilities that entities should implement, regardless of its size, industry or geography. These foundational practices are part of the SCF's Cybersecurity Oversight, Resilience and Enablement (SCF CORE) Fundamentals baseline, designed to:

(1) Contain administrative, technical and physical safeguards for the protection of Technology Assets, Applications, Services and/or Data (TAASD); and
(2) Protect against any reasonable risks and threats.

From a due care perspective, an entity is expected to demonstrate conformity with the following practices:

12.1 Ability To Demonstrate Conformity

The entity must ensure it is able to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.

Relevant SCF Control(s):
- CPL-01.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A capability exists to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.
(2) Personnel or roles to whom the assignment of being able to demonstrate conformity is assigned.

12.1.1 Conformity Assessment

The entity must conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.

Relevant SCF Control(s):
- CPL-01.4

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Assessments are conducted to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.

12.1.2 Cybersecurity & Data Protection Status Reporting

The entity must submit status reporting of its cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.

Relevant SCF Control(s):
- GOV-19

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The basis for confidence that implemented practices conform to applicable security, compliance and resilience controls, where the control implementation performs as intended is defined.

12.2 Non-Compliance Oversight

The entity must document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.

Relevant SCF Control(s):
- CPL-01.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Instances of non-compliance with statutory, regulatory and/or contractual obligations are:
   a. Documented, including the reason(s) for non-compliance;
   b. Formally-reviewed;
   c. Centrally-governed to maintain appropriate situational awareness; and
   d. Assigned to individuals or teams for remediation.

(2) Remediation plans for instances of non-compliance with statutory, regulatory and/or contractual obligations are documented.

12.2.1 Monitor Controls

The entity must compel data and/or process owners to monitor Technology Assets, Applications and/or Services (TAAS) under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity and data protection controls are operating as intended.

Relevant SCF Control(s):
- GOV-15.5

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) 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 / data privacy controls are operating as intended.

(2) 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 / data privacy controls are operating as intended.

12.2.2 Periodic Audits

The entity must conduct periodic audits of cybersecurity and data protection controls to evaluate conformity with its documented policies, standards and procedures.

Relevant SCF Control(s):
- CPL-02.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The entity conducts periodic, formal audits of cybersecurity & data protection controls for conformity with the entity's policies, standards and procedures.

(2) Personnel or roles to whom the assignment conformity assessments are assigned.

12.2.3 Functional Review Of Cybersecurity & Data Protection Controls

The entity must regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to its cybersecurity and data protection policies and standards.

Relevant SCF Control(s):
- CPL-03.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) *Controls are assessed in the system and its environment of operation per an entity-defined 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 and/or data privacy requirements.*
(2) *A control assessment report is produced that documents the results of the assessment.*
(3) *The results of the control assessment are provided to individuals or roles.*

12.2.4 Third-Party Scope Review

The entity must perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.

Relevant SCF Control(s):
- TPM-05.5

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, is performed to ensure cybersecurity / data privacy control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.*
(2) *Processes, methods and techniques to monitor security requirement compliance by external service providers on an ongoing basis are implemented.*

12.2.5 Review of Third-Party Services

The entity must monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.

Relevant SCF Control(s):
- TPM-08

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *The frequency at which to assess and review the supply chain-related risks associated with suppliers or contractors and the systems, system components or system services they provide is defined.*
(2) *The supply chain-related risks associated with suppliers or contractors and the systems, system components or system services they provide are assessed and reviewed per an entity-defined frequency.*

12.2.6 Managing Changes To Third-Party Services

The entity must control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.

Relevant SCF Control(s):
- TPM-10

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:
(1) *Affected third-parties are identified through change control practices.*
(2) *Provided services are assessed for impact from proposed changes.*
(3) *Recurring reviews are performed of third-party provided services against existing contract requirements.*
(4) *Discrepancies in services provided and/or geolocation of provided services are evaluated for impact to the entity's operations.*

12.3 Measures of Performance

The entity must develop, report and monitor cybersecurity and data protection program measures of performance.

Relevant SCF Control(s):
- GOV-05

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Cybersecurity and data privacy measures of performance are:
   a. Developed; and
   b. Monitored.

(2) The results of cybersecurity and data protection measures of performance are reported.

12.3.1 Key Performance Indicators (KPIs)

The entity must develop, report and monitor Key Performance Indicators (KPIs) to assist executive leadership in performance monitoring and trend analysis of the cybersecurity and data protection program.

Relevant SCF Control(s):
- GOV-05.1

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Key Performance Indicators (KPIs) are developed to assist executive leadership in performance monitoring and trend analysis of specific aspects of the entity's cybersecurity and data protection program.

12.3.2 Key Risk Indicators (KRIs)

The entity must develop, report and monitor Key Risk Indicators (KRIs) to assist executive leadership in performance monitoring and trend analysis of the cybersecurity and data protection program.

Relevant SCF Control(s):
- GOV-05.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Key Risk Indicators (KRIs) are developed to assist executive leadership in performance monitoring and trend analysis of specific aspects of the entity's cybersecurity and data protection program.

12.4 Incident Response Testing

The entity must formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.

Relevant SCF Control(s):
- IRO-06

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The frequency at which to test the effectiveness of the incident response capability for the system is defined.

(2) Tests used to test the effectiveness of the incident response capability for the system are defined.

(3) The effectiveness of the incident response capability is tested per an entity-defined frequency.

(4) Intrusion-monitoring tools and mechanisms are tested frequently.

12.4.1 Monitoring For Indicators of Compromise (IOC)

The entity must monitor for and alert on Indicators of Compromise (IoC).

Relevant SCF Control(s):
- BCD-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) Anomalous or suspicious behavior is defined.
(2) IOC are defined.
(3) Sources that provide Indicators of Compromise (IOC) are defined.
(4) IOC provided by sources are discovered.
(5) IOC provided by sources are collected.
(6) Unauthorized use of the system is identified through techniques and methods.

12.4.2 Contingency Plan Testing & Exercises

The entity must conduct tests and/or exercises to evaluate the contingency plan's effectiveness and its readiness to execute the plan.

Relevant SCF Control(s):
- BCD-04

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The frequency of testing the contingency plan for the system is defined.
(2) Tests for determining the effectiveness of the contingency plan are defined.
(3) Tests for determining readiness to execute the contingency plan are defined.
(4) The contingency plan for the system is tested frequently.

12.5 Commitment To Continual Improvements

The entity must commit appropriate resources needed for continual improvement of the entity's cybersecurity and data protection program, including:

(1) Staffing;
(2) Budget;
(3) Processes; and
(4) Technologies.

Relevant SCF Control(s):
- GOV-01.3

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The entity commits appropriate financial resources needed for continual improvement of the entity's cybersecurity & data privacy program.

12.5.1 Status Reporting To Governing Body

The entity must provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to its cybersecurity and data protection program.

Relevant SCF Control(s):
- GOV-01.2

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) The executive steering committee, or advisory board, makes executive decisions about matters considered material to the entity's cybersecurity and data protection program.

12.6 Quality Management System (QMS)

The entity must govern a Quality Management System (QMS) to ensure cybersecurity and data protection processes conform with applicable statutory, regulatory and/or contractual obligations.

Relevant SCF Control(s):

- GOV-18

NOTE: To demonstrate conformity with this requirement, in addition to relevant policies, standards and procedures, the entity needs sufficient evidence to support control effectiveness claims that can prove:

(1) A Quality Management System (QMS) is implemented to ensure cybersecurity and data protection processes conform with applicable statutory, regulatory and/or contractual obligations.

13 DEMONSTRATING ASSURANCE TO STAKEHOLDERS

Regardless of the industry, there is a definitive need for a third-party verified certification that assesses tailored cybersecurity and data protection controls that could impact an entity and its supply chain stakeholders. The SCRMS was designed to integrate with the SCF's conformity assessment program that is designed to provide third-party validation of an entity's security, compliance and resilience controls.

13.1 SECURITY, COMPLIANCE & RESILIENCE CONFORMITY ASSESSMENT PROGRAM (SCR CAP)

The Security, Compliance & Resilience Conformity Assessment Program (SCR CAP) can be used to demonstrate assurance to stakeholders, since it is an entity-level conformity assessment.[27]

The SCR CAP is designed to utilize tailored cybersecurity and privacy controls that specifically address the applicable statutory, regulatory and contractual obligations an Organization Seeking Assessment (OSA) is required to comply with. By using the metaframework nature of the SCF, an OSA is able to perform conformity assessment that spans multiple cybersecurity and privacy-specific laws, regulations and frameworks.

The SCR CAP is focused on using the SCF as the control set to provide a company-level certification. While the SCR CAP shares some similarities with other existing, single-focused certifications (e.g., ISO 27001, CMMC, FedRAMP, etc.), the SCR CAP is unique in its metaframework approach to covering cybersecurity and data protection requirements that span multiple laws, regulations and frameworks.

As cybersecurity and data protection operations are multi-faceted, the SCR CAP is designed to ensure that assessed controls reflect the real-world requirements faced by the OSA from a statutory, regulatory and contractual perspective. An assessment that only covers a part of an OSA's cybersecurity and data protection program results in an inaccurate and incomplete report on the OSA's overall security posture, providing a false sense of security to the OSA.

The SCR CAP is designed for cybersecurity & privacy practitioners by cybersecurity & data privacy practitioners. This concept is based on the need within the industry for a tailored conformity assessment solution that is capable of addressing several key considerations:

- View compliance as a natural by-product of secure practices;
- Scale to address multifaceted operational requirements (e.g., laws, regulations and frameworks);
- Acknowledge the stated risk tolerance of the OSA since not all entities have the same risk tolerance;
- Minimize the risk of "gaming" the certification process that provides no useful insights into the security posture of the OSA;
- Utilize technology to make the assessment process more efficient to drive down labor-related assessment costs; and
- Leverage existing industry recognized practices, where possible.

13.2 SCF CERTIFICATION OPTIONS

To learn more about SCF certification options, please contact the SCF at https://securecontrolsframework.com/contact-us/

Earning a SCF Certified™ conformity designation is meant to signify an accomplishment, rather than be viewed as a "participation ribbon" that has little practical value for the OSA or stakeholders in the OSA's supply chain to understand the OSA's security posture.

[27] *Security, Compliance & Resilience Conformity Assessment Program (SCR CAP) - https://securecontrolsframework.com/training-certifications/scf-certifications/scf-conformity-assessment-program-cap/*

ERRATA

2026.1

- Initial documentation published

CONTRIBUTOR ACKNOWLEDGEMENT

The Secure Controls Framework Council wants to thank these individuals for their contributions in the development and refinement of the Security Compliance & Resilience Management System (SCRMS):

- Tom Cornelius, SCF Council
- Andy Kuykendall, SCF Council
- Adam German, SCF Council
- Kimberly Owen, SCF Council
- Jason Sproesser, SCF Council
- William Birchett, Logos Systems
- Scott Alldridge, IP Services
- Robert Hill, Cyturus Technologies
- Keren de Via, Cyturus Technologies
- Joshua Marpet, Cyturus Technologies
- Steven Mancini
- Joy Beland, Summit7
- David Driggers, SCF Connect
- Dave Schmoeller, SCF Connect
- Michael Parisi, Steel Patriot Partners
- Mike Snyder, Cyber AB
- Adam Glover, Insight Assurance

ANNEXES

ANNEX 1: APPLICABLE SECURE CONTROLS FRAMEWORK (SCF) CONTROLS

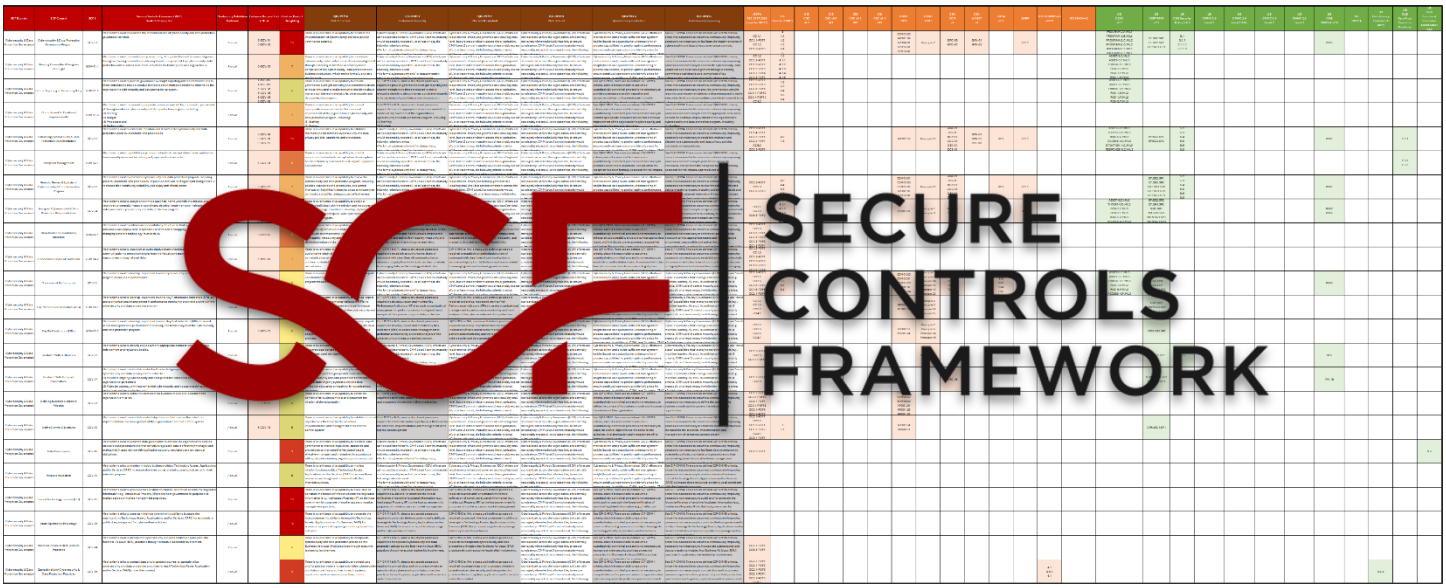
The following Secure Controls Framework (SCF) controls are mapped into the SCRMS for due diligence and due care activities (sections 11 and 12 of the SCRMS).

The controls that make up the SCRMS:

(1) Should be considered a discussion starting point for medium to enterprise sized entities to define what it means to be secure, compliant and resilient; and

(2) Are selected for reasonableness. While certain controls may be not applicable (e.g., embedded technology), the expectation is most will be applicable for larger entities.

The SCRMS column in the SCF is designed to start the discussion for tailoring purposes, where there may be more or less applicable controls once an entity thoroughly analyzes its needs for security, compliance and resilience capabilities.



Note: The SCF is free to download.[28] The column containing SCRMS controls is labelled "SCF SCRMS" on the main SCF tab.

[28] *Secure Controls Framework (SCF) Download - https://securecontrolsframework.com/free-scf-content/scf-download/*

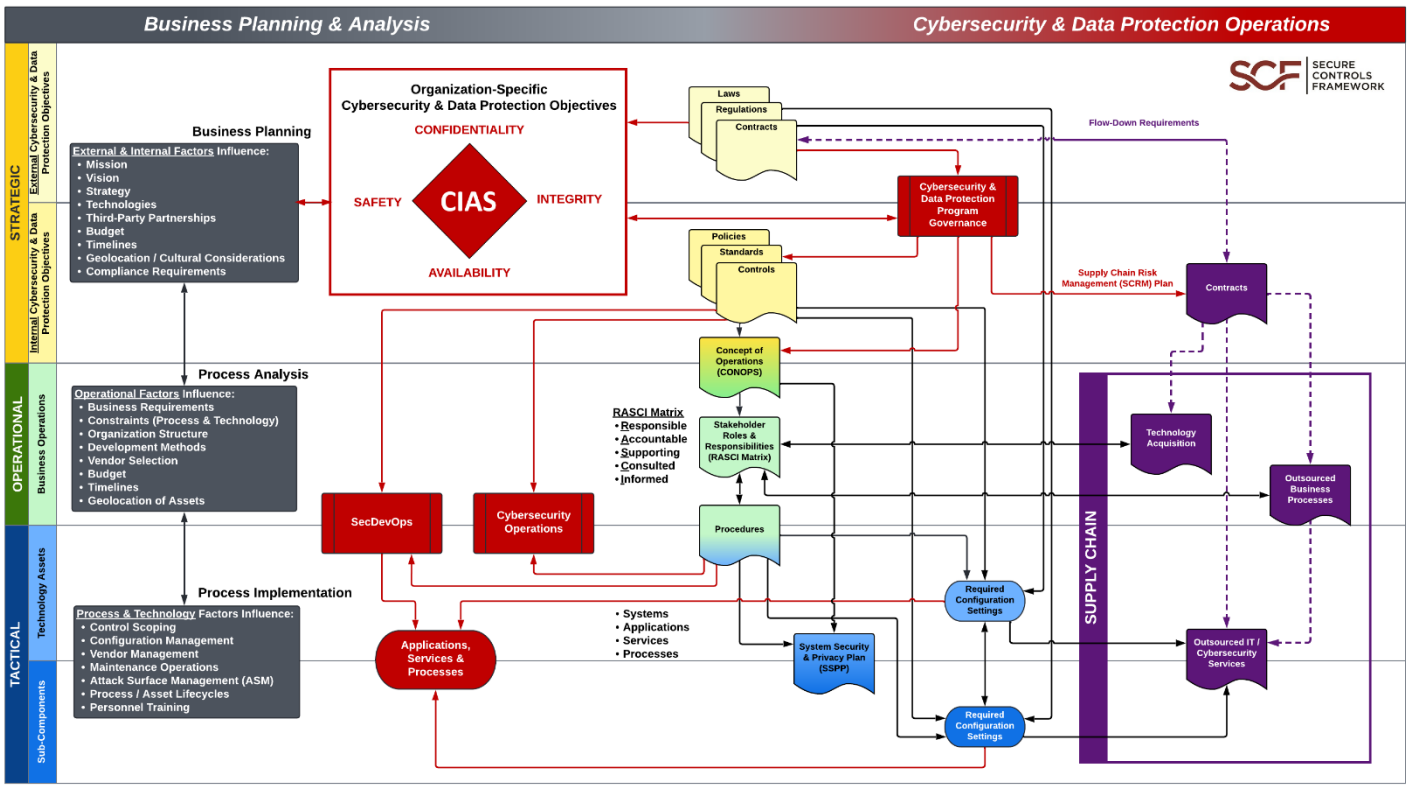
ANNEX 2: ADEQUATE SECURITY

The SCRMS recognizes that no technology can provide "absolute security" due to the limits of human certainty. This uncertainty exists in the lifecycle of every system, application and/or product and is often due to the constraints of cost, schedule, performance, feasibility and practicality. Therefore, trade-offs must be routinely made across contradictory, competing and conflicting needs and limitations. However, these trade-offs must be optimized to achieve "adequate security," reflecting a risk-based decision by stakeholders. [29]

The SCRMS leverages concepts from NIST SP 800-160 and other guidance to explain the holistic concepts of how broader business planning and analysis ultimately lead to actionable cybersecurity and/or data protection requirements. Understanding this hierarchical nature of requirements is a fundamental construct of cybersecurity and/or data protection control governance processes.

This concept is depicted in the following graphic for how the concept of adequate security is based on business planning and analysis as it relates to establishing protection requirements: [30]

Hierarchical Methodology To Determine "Adequate Security" To Build Secure, Resilient & Compliant Systems and Processes



An entity publishes policies to eliminate potential gaps in that desired governed behavior to achieve "adequate security" based on what a reasonable individual would be expected to do in a similar situation. The rules associated with this "governed behavior" must be accurate, consistent, compatible and complete with respect to the executive leadership's objectives to accomplish the entity's mission and overall strategy.

An entity's policies ultimately define the behavior of Individual Contributors (IC) (e.g., engineers, analysts, developers, etc.) in performing their roles and associated responsibilities for developing processes and procedures. This eventually leads to the configuration of technology assets (e.g., systems, applications, services and processes), where a discrete set of restrictions and properties must exist to specify how that asset enforces or contributes to implementing an entity's security policies.

[29] *NIST SP 800-160 Vol 1 Rev 1 Appendix C - https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final*
[30] *SCF Adequate Security Determination Process - https://securecontrolsframework.com/content/adequate-cybersecurity-methodology.pdf*

The required configuration settings for technology assets must include technical and business requirements, which ultimately fall under an entity's cybersecurity and/or data protection policies. Requirements can be categorized as follows: [31]

- Stakeholder requirements that address the need to be satisfied in a design-independent manner; and
- System requirements express the specific solution that will be delivered in a design-dependent manner.

A2.1: Establishing Secure Systems

A "secure system" is a system that ensures that only the authorized intended behaviors and outcomes occur, thereby providing freedom from those conditions, both intentionally/with malice and unintentionally/without malice, that can cause a loss of information assets with unacceptable consequences.[32] This definition expresses an ideal that captures three (3) essential aspects of what it means to achieve security:

(1) Enable the delivery of the required system capability despite intentional and unintentional forms of adversity;
(2) Enforce constraints to ensure that only the desired behaviors and outcomes associated with the required system capability are realized while satisfying the first aspect; and
(3) Enforce constraints based on rules to ensure that only authorized human-to-machine and machine-to-machine interactions and operations are allowed to occur, while satisfying the second aspect.

For a system, adequate security is an evidence-based determination that achieves and optimizes security performance against all other performance objectives and constraints. Judgments of adequate security are driven by the stakeholder objectives, needs and concerns associated with the system. Adequate security has two elements:

- Achieve the minimum acceptable threshold of security performance; and
- Maximize security performance to the extent that any additional increase in security performance degrades some other aspects of system performance or requires an unacceptable operational commitment.

A2.2: Defining Stakeholder Security Requirements

Stakeholder security requirements are those stakeholder requirements that are security-relevant. Stakeholder security requirements specify:

- The protection needed for the mission or business, data, information, processes, functions, human and system assets;
- The roles, responsibilities and security-relevant actions of individuals who perform and support the mission or business processes;
- The interactions between the security-relevant solution elements; and
- The assurance that is to be obtained in the security solution.

A2.3: Defining System Security Requirements

System requirements specify the technical view of a system or solution that meets the identified stakeholder needs. The system requirements are a transformation of the validated stakeholder requirements. System requirements specify what the system or solution must do to satisfy the stakeholder requirements. System security requirements are those system requirements that are security relevant. These requirements define:

- The protection capabilities provided by the security solution;
- The performance and behavioral characteristics exhibited by the security solution;
- Assurance processes, procedures and techniques;
- Constraints on the system and the processes, methods and tools used to realize the system; and
- The evidence required to determine the system security requirements have been satisfied.

[31] *NIST SP 800-160 Vol 1 Rev 1 Appendix C - https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final*
[32] *NIST SP 800-160 Vol 1 Rev 1 - https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final*

A2.4 System of Systems (SoS) Engineering

A system is *"an arrangement of parts or elements that together exhibit a behavior or meaning that the individual constituents do not."*[33] Since engineers/architects/developers do not design, code and maintain Applications, Services and Processes (ASP) in a vacuum, they need to embrace a "system of systems" mindset toward system interaction since there are legitimate cybersecurity and/or data protection concerns with untrustworthy dependencies. A system of systems is a *"set of systems and system elements interacting to provide a unique capability that none of the constituent systems can accomplish on their own."*[34] A system of systems consists of several constituent systems plus any inter-system infrastructure, facilities and processes necessary to enable the constituent systems to integrate or interoperate.

This concept includes "interfacing systems" that have an interface for exchanging data or information, energy, or other resources. Interfacing systems have two specific subsets:

- Enabling Systems. These provide essential services required to create and sustain the system. Examples of enabling systems include:
  - Development environments;
  - Production systems, applications and services;
  - Training systems; and
  - Maintenance systems; and
- Interoperating Systems. These interact with systems to jointly perform a function during the utilization and sustainment stages of the system life cycle. Interoperating systems often form a system of systems.
- Sustainability – SoS imposes sustainability of legacy systems as newer systems evolve.

[33] *NIST SP 800-160 Vol 1 Rev 1 - https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final*
[34] *NIST SP 800-160 Vol 1 Rev 1 - https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final*

ANNEX 3: DEFENSIBLE EVIDENCE

Defensible evidence is a multifaceted concept, where it goes beyond having documented policies, standards and procedures. This section provides guidance on the types of evidence an entity should plan for to demonstrate secure, compliant and resilient capabilities.

A3.1: GOVERNANCE EVIDENCE

The objective of governance evidence is to clearly demonstrate executive leadership oversight and accountability.

Examples include the following types of documentation:

- Cybersecurity program charter.
- Cybersecurity strategy.
- Quarterly Business Review (QBR) briefing materials.
- Security steering committee minutes.
- Policies and standards.

A3.2: RISK EVIDENCE

The objective of risk evidence is to clearly demonstrate risks were identified and managed.

Examples include the following types of documentation:

- Risk Management Program (RMP).
- Supply Chain Risk Management (SCRM) plan.
- Formal risk assessments.
- Data Protection Impact Assessments (DPIAs).
- Threat intelligence feeds.
- Threat catalog.
- Entity-specific threat analysis.
- Risk catalog.
- Risk register or Plan of Action & Milestones (POA&M).
- Control gap analysis.
- Risk acceptance documentation.

A3.3: SECURITY CAPABILITY EVIDENCE

The objective of security capability evidence is to clearly demonstrate appropriately scoped controls exist and operate effectively.

Examples include the following types of documentation:

- Documented policies, standards and procedures.
- System Security Plan (SSP) or similar documentation.
- Secure Baseline Configurations (SBC) for deployed technology assets.
- IT Asset Management (ITAM) program.
- Identity and Access Management (IAM) program.
- Incident Response Plans (IRPs).
- Security event monitoring.
- Vulnerability and Patch Management Program (VPMP).
- Vulnerability assessment scans.

A3.4: COMPLIANCE EVIDENCE

The objective of compliance evidence is to clearly demonstrate conformity with statutory, regulatory and/or contractual obligations.

Examples include the following types of documentation:

- Identification of applicable laws, regulations and/or contracts with entity-specific compliance obligations.
- Conformity with one or more cybersecurity frameworks, if applicable.
- Results from assessments / audits.
- Evidence of how instances of non-conformity are governed (e.g., compensating controls).
- Plan of Action & Milestones (POA&M) to govern instances of non-conformity.

A3.5: Resilience Evidence

The objective of resilience evidence is to clearly demonstrate that the entity is reasonably capable of recovering from incidents.

Examples include the following types of documentation:

- Incident response reports.
- Evidence of actions taken from Root Cause Analysis (RCA) after incidents.
- Incident response exercises.
- Disaster recovery tests.
- Business continuity exercises.

A3.6: Assurance Evidence

The objective of assurance evidence is to clearly demonstrate independent validation of the entity's cybersecurity program.

Examples include the following types of documentation:

- Third-party audits.
- Penetration testing.
- Reports from regulatory inspections.

ANNEX 4: PLANNING FOR RESISTANCE

From a legal defensibility and professional ethics standpoint, a CISO must be able to demonstrate evidence of both due diligence and due care:

- Due Diligence. The level of reasonable care or attention expected to avoid liability. [35]
- Due Care. The standard of care where a reasonable person would exercise in the same situation or under similar circumstances. This standard of care is used in a tort action to determine whether a person was negligent. [36]

A defensible position for a CISO is the ability to state: *"The entity's leadership was informed of the risk, the controls were recommended, and leadership knowingly accepted the risk."* The CISO's job is to ensure that statement is provable through defensible evidence.

A reasonable assumption for a CISO is that at some point the CEO or board will refuse to fund one, or more, necessary cybersecurity capabilities. In this scenario, the CISO's priority should temporarily shift to creating a defensible record showing that the entity's leadership knowingly accepted the risk. The reason for this is to protect the CISO from accusations of negligence from:

- Incidents (malicious or accidental);
- Regulatory inquiries;
- Insurance claim investigations;
- Lawsuits (e.g., shareholder, class action, breach of contract, etc.); and
- Whistleblower claims (e.g., qui tam actions).

To avoid personal liability, a CISO may resign before a foreseeable, catastrophic event occurs. However, leaving before a catastrophic incident does not necessarily remove that individual from scrutiny, since after a significant incident, investigators typically ask historically-relevant questions:

(1) Was risk identified?
(2) Was leadership informed?
(3) Were reasonable controls recommended?
(4) Did leadership knowingly accept risk?

For an individual serving in the role of a CISO to have evidence to back up affirmative answers to those questions, that should withstand scrutiny. Therefore, a prudent CISO will adhere to the following guidance to maintain necessary defensible evidence:

A4.1: FORMAL CYBERSECURITY STRATEGY & IMPLEMENTATION PLAN

The first line of defense for a CISO is to demonstrate a credible plan that aligned with industry-recognized secure practices.

Evidence of this can be demonstrated through the following documentation:

(1) Formal cybersecurity strategy (e.g., 3–5 year roadmap).
(2) Budget requests to implement the strategy.
(3) Prioritized objectives to operationalize the strategy (e.g., implementation roadmap).
(4) Assigned objectives to roles/individuals within the cybersecurity department.
(5) Status reports on the state of strategy rollout.

This demonstrates proactive leadership by the CISO, where the CISO:

- Performed due diligence to identify security, compliance and resilience needs at the tactical, operational and strategic levels;
- Leveraged recognized standards for reasonable care;
- Identified capability gaps; and
- Proposed reasonable solutions.

A4.2: DOCUMENTED RISK ASSESSMENTS AND BUSINESS IMPACT ASSESSMENTS (BIAS)

The entity's executive leadership will not be able to reasonably claim ignorance if the CISO clearly quantifies and documents risk.

Evidence of this can be demonstrated through the following documentation:

(1) Formal risk assessments, including:
    a. Data Protection Impact Assessment (DPIAs); and

[35] *Cornell Law School Legal Information Institute - https://www.law.cornell.edu/wex/due_diligence*
[36] *Cornell Law School Legal Information Institute - https://www.law.cornell.edu/wex/due_care*

b. Supply Chain Risk Assessment (SCRAs).

(2) Business Impact Analysis (BIA).
(3) Threat modeling and attack scenarios.
(4) Supply Chain Risk Management (SCRM) plan.

Using clear language that executives understand, the CISO can provide necessary context:

- Financial loss;
- Regulatory exposure;
- Operational downtime; and
- Safety impact.

A4.3: Formal Risk Register

The entity's risk register is one of the strongest pieces of defensible evidence for a CISO. This must be properly maintained to ensure its integrity (e.g., immutable date/time stamp entries).

At a minimum, risk registers should contain the following components:

(1) Risk description.
(2) Likelihood.
(3) Impact (including non-compliance with statutory, regulatory and/or contractual obligations).
(4) Affected assets.
(5) Recommended controls and/or compensating controls.
(6) Estimated remediation cost and timeline.
(7) Risk owner.
(8) Risk acceptance status.

A4.4: Incidents Tracking

Incidents are often the catalyst for broader scrutiny. Directly linking incidents to unfunded capabilities provides evidence for the CISO to justify budget for necessary capabilities (e.g., tooling, staffing, training, etc.).

Evidence of this can be demonstrated through the following documentation:

(1) Attempted attacks that were prevented.
(2) Incidents that occurred.
(3) Phishing campaigns.
(4) Penetration test findings.

A4.5: Third-Party Assessments

External validation significantly strengthens defensibility. Recommendations from independent experts can often help a CISO justify budget requests and capabilities prioritization.

Evidence of this can be demonstrated through the following documentation:

(1) Third-party assessments.
(2) Penetration testing.
(3) Compliance audit.
(4) Maturity assessments.

If executive leadership ignores independent expert advice, the CISO is better protected through clearly stated:

- Capability gaps;
- Recommended controls; and
- Risk exposure.

A4.6: Document Decisions

A "CISO Journal" should be maintained to serve as a structured log of the CISO's analysis and decisions. This type of evidence may be extremely valuable during litigation or other investigations, since it provides a chronological journal of the CISO's thoughts and actions, including stakeholder interactions (e.g., meeting with CEO on X date where the CEO delayed breach detection capability for XYZ reason).

In addition to a personal journal, CISOs should maintain copies of:

(1) Strategy documents.
(2) Risk assessments.
(3) Board presentations.
(4) Budget requests.
(5) Rejected initiatives.
(6) Escalation communications.

In employment ends after an incident, this documentation serves as personal professional protection. Based on the sensitive nature of the documentation, this may involve the CISO emailing the evidence back to the CISO's work email, so it is capable of being found during eDiscovery.

A4.7: Reporting Risk To Executive Leadership

CISOs should ensure security, compliance and resilience topics appear in board reporting.

Evidence of this can be demonstrated through the following documentation:

(1) Quarterly Business Review (QBR) board briefings.
(2) Risk committee presentations.
(3) Audit committee presentations.
(4) Cybersecurity dashboards.
(5) Other executive leadership-focused security program updates.

If executive leadership knowingly exposes the entity to illegal or catastrophic risk, professional options for the CISO include:

- Escalating to the board audit committee;
- Involving internal audit;
- Seeking legal counsel;
- Resigning with documented concerns; and
- Whistleblower submissions (e.g., appropriate law enforcement or False Claims Act qui tam actions).

A4.8: Formal Risk Acceptance from Leadership

The goal is documented executive accountability, since the role of the CISO is not meant to own the risk. Escalation should always be documented in writing. If executives refuse funding, the CISO should require written risk acceptance.

A typical escalation path for a CISO is:

(1) CIO.
(2) Executive leadership (e.g., CFO, COO, CEO, etc.).
(3) Board-level risk committee.
(4) Board-level audit committee.

Methods of documenting risk acceptance include, but are not limited to:

- Risk Acceptance Form (RAF). A RAF would be signed by one, or more, executives, where risk is formally acknowledged.
  - *Note: While this appears to be the most optimal method, it is politically dangerous to the CISO.*
- Board meeting minutes. This is a neutral method for existing meeting minutes to capture the discussion and outcome.
  - *Note: This assumes board meeting minutes capture necessary details.*
- Email summary. A clear, concise email is sent to the individual, or individuals, to document the conversation that summarizes the risk, the request and the reason for the refusal.
  - *Note: The email summary is designed to be found during eDiscovery.*

A4.9: Preserve Evidence of Professional Competence

Maintain documentation of professional competence in the role of the CISO.

Evidence of this can be demonstrated through the following documentation:

(1) Properly scoped policies and standards.
(2) Security architecture that is aligned with industry-recognized secure practices.

(3) Implementation of Secure Baseline Configurations (SBC).
(4) Tested and viable incident response capabilities.
(5) Recurring security training that encourages business-as-usual secure practices.
(6) Proactive risk management program.
(7) Proactive vulnerability management program.

This type of evidence can clearly demonstrate the CISO acted reasonably with available resources.