SECURE CONTROLS FRAMEWORK

PRIORITIZED IMPLEMENTATION GUIDE

Security, Compliance & Resilience Management System Prioritized Implementation Guide (SCRMS-PIG)

Version 2026.1

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

Table of Contents

NOTE: 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.

EXECUTIVE SUMMARY

The **Security, Compliance & Resilience Management System (SCRMS)** is a governance-driven management system designed to help entities design, implement, operate and oversee capabilities that are secure, compliant and resilient.[1] The SCRMS is designed to:

- Withstand regulatory, contractual and litigation scrutiny; and
- Be applicable across the entity's **People, Processes, Technologies, Data & Facilities (PPTDF)**.

Compliance is viewed as a natural byproduct of secure and resilient processes, where certifications and audit readiness are outputs of operational discipline, not drivers of it. This prioritizes risk and threat management capabilities to increase stakeholder confidence in the entity's capabilities through the ability to demonstrate assurance with defensible evidence of due diligence and due care practices.

The SCRMS is framework-agnostic and technology-neutral. It does not replace existing standards or regulations. Instead, the SCRMS provides a unifying operational structure that allows entities to consistently meet statutory, regulatory, contractual requirements, in addition to discretionary risk-based security and resilience expectations, in a reasonable and defensible manner.

At its core, the SCRMS exists to answer a single question that stakeholders want to know (e.g., customers, shareholders, regulators, auditors, insurers, etc.): *"Is the entity acting reasonably to protect its mission, data and operations?"*

PRIORITIZED IMPLEMENTATION GUIDANCE

The **SCRMS Prioritized Implementation Guide (SCRMS-PIG)** is the operational companion to the SCRMS. It provides a sequenced, dependency-aware roadmap for implementing SCRMS capabilities in a way that:

- Supports the entity's mission and business practices;
- Avoids rework from implementing capabilities where dependencies exist that results in cascading failures from misaligned PPTDF;
- Aligns funding and resources with business risk;
- Avoids systemic weaknesses by building foundational capabilities before chasing advanced capabilities; and
- Provides assurance to stakeholders through audit-ready evidence.

The SCRMS is not about perfect security. It is about reasonable, defensible and governable security, compliance and resilience that is designed to withstand scrutiny and support the entity's mission over time. The SCRMS-PIG makes that outcome achievable, measurable and sustainable.

The SCRMS-PIG breaks down control implementation into thirty (30) major steps, which can then be translated into a viable project plan.

- Twenty-six (26) steps are focused on due diligence activities; and
- Four (4) steps are focused on due care activities.

The structure of the SCRMS-PIG is designed to support:

- Strategic decision-making
- Budget justification for cybersecurity and data protection capabilities;
- Deficiency remediation; and
- Audit readiness is a byproduct of defensible governance.

[1] SCRMS - https://securecontrolsframework.com/free-content/security-compliance-resilience-management-system-scrms

Why The SCRMS Exists

Entities rarely fail because they lack controls. Failures often occur because leadership cannot prove:

- Reasonable prioritization; or
- Evidence of oversight after the fact.

The SCRMS addresses these gaps by:

- Aligning cybersecurity and data protection capabilities with **Enterprise Risk Management (ERM)**;
- Separating execution (management) from oversight (executive and board); and
- Producing defensible evidence of both due diligence and due care activities.

What Makes The SCRMS Different

The SCRMS is built to model material risk and material control failure.

The SCRMS was purpose-built for real-world accountability, not checklist compliance. 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.

The SCRMS is intended to be utilized as a holistic, technology-agnostic framework for an entity to design, implement and maintain secure, compliant and resilient capabilities, covering an entity's PPTDF, regardless of how or where data is stored, processed and/or transmitted. All such expectations are operationalized and governed through the entity's **Living Control Set (LCS)**, which defines what "reasonable" means for that entity at a given point in time.

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 LCS capable of adjusting to specific security, compliance and resilience requirements that it must address.

The SCRMS is equally applicable whether an entity is:

- Establishing a program from scratch;
- Rationalizing overlapping compliance obligations; and/or
- Demonstrating reasonable security to external stakeholders.

Value To Executives and Board Members

By adopting SCRMS and the SCRMS-PIG, an entity's leadership gains:

- Clear visibility into risk posture;
- Documented oversight and accountability;
- Evidence of reasonable decision-making;
- Confidence in legally defensible evidence of conformity; and
- A shared language between business, risk, legal and technical stakeholders

Most importantly, the SCRMS allows leadership to credibly demonstrate: *"We understand our risks, we prioritize them rationally and we continuously adapt our capabilities as conditions change."*

SCRMS Prioritized Implementation Plan (SCRMS-PIG)

The SCRMS-PIG was approached from the perspective of, *"If I was hired at a company, what would my plan be to start from nothing to get a company to where it could successfully implement the SCRMS?"*

While all **Secure Controls Framework (SCF)** controls identified within the SCRMS are addressed within the SCRMS-PIG, it is important to note that the prioritization of capabilities into unique steps is a subjective endeavor and not everyone may agree with this approach. Therefore, it is important to understand that every entity is different and an implementer (e.g., cybersecurity practitioner) will invariably need to modify the approach to fit the entity's specific needs.

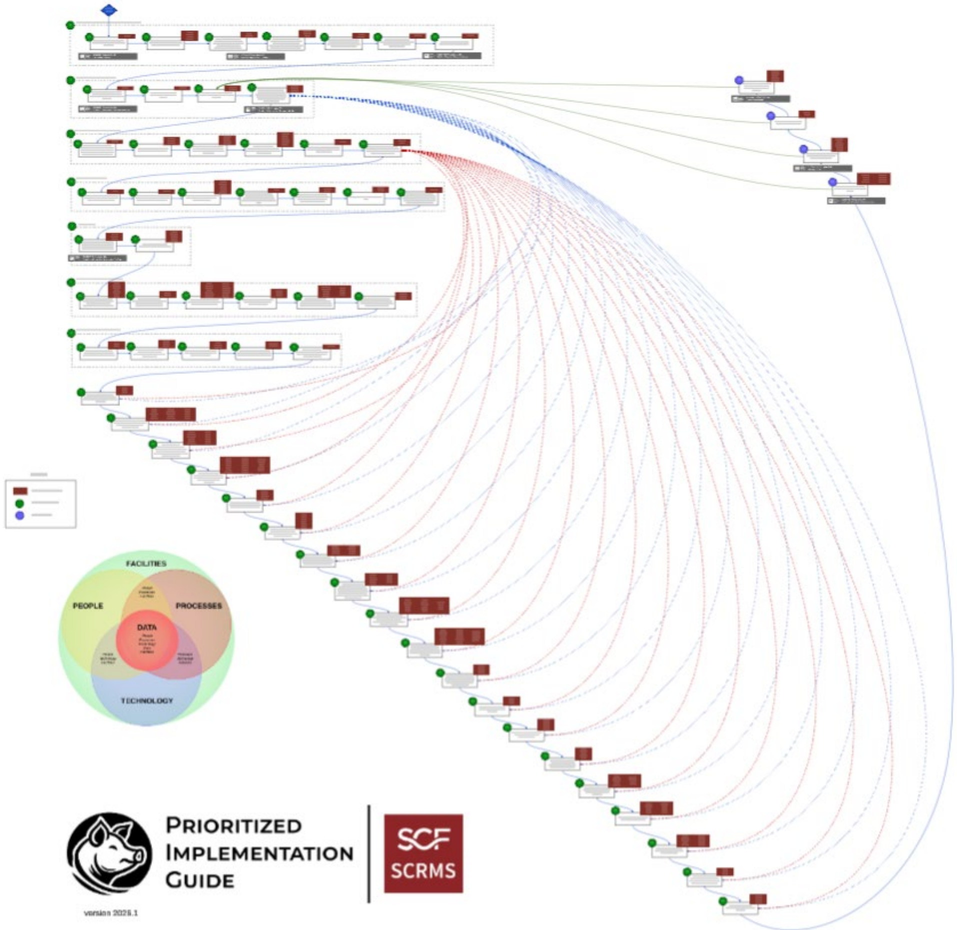
The SCRMS-PIG is designed to provide a roadmap that would be usable for anyone:

(1) Starting out new with the SCRMS; or
(2) Wanting to double check their approach to the SCRMS.

NOTE: The steps in the SCRMS-PIG are not purely linear. The sequencing establishes dependency logic, but risk thresholds, materiality and business conditions may reprioritize efforts dynamically.

SCRMS-PIG Flowchart

The SCRMS-PIG flowchart graphic is available for download by clicking on the image below (PDF format):[2]



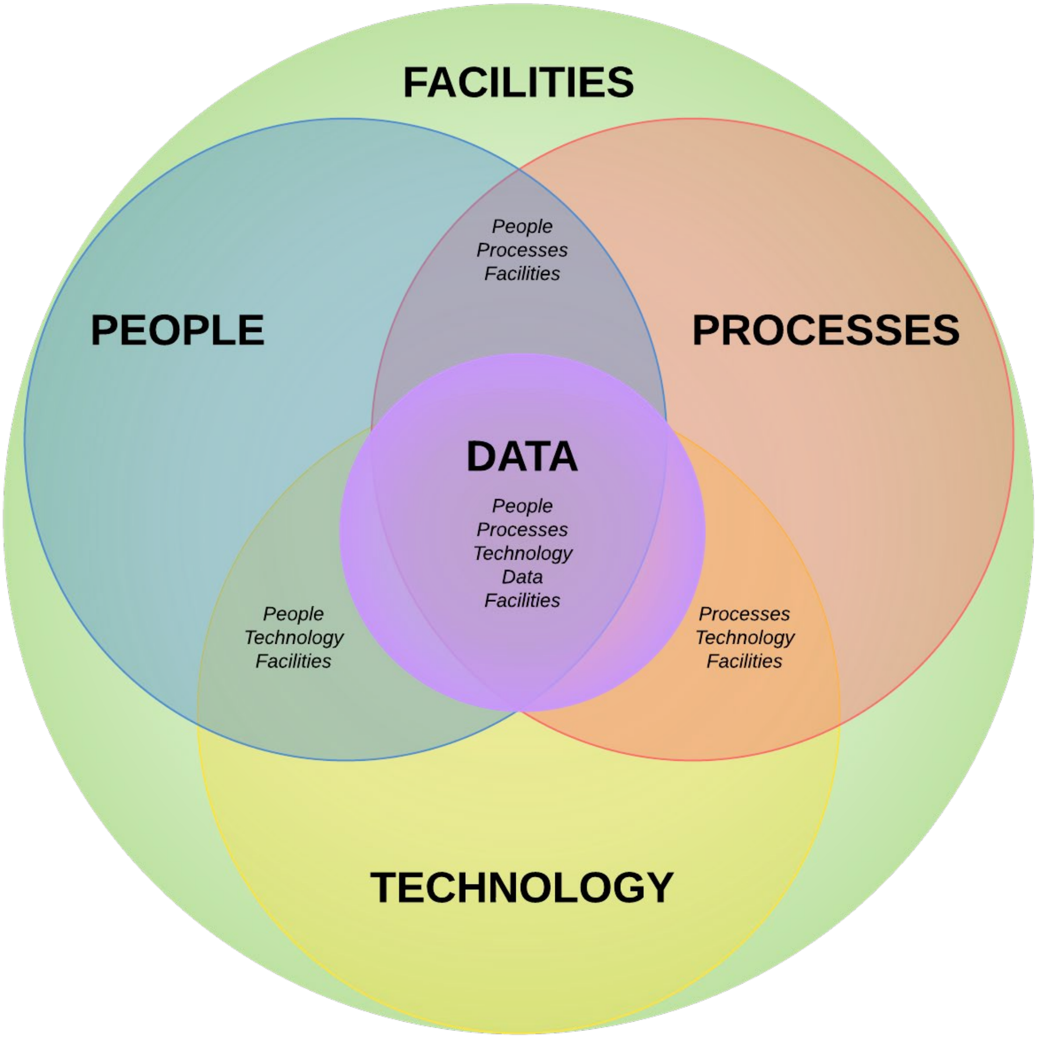
[2] SCRM-PIG Flowchart - https://securecontrolsframework.com/content/scrms-pig-flowchart.pdf

People, Processes, Technologies, Data & Facilities (PPTDF) Applicability

Appendix A – SCRMS Controls Prioritization identifies PPTDF applicability at the control level to assist with understanding what is the focus of the control implementation.

The 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.).



Defensible Governance Utilizing Due Diligence & Due Care

The SCRMS defines what it means to be secure, compliant and resilient in a holistic, framework-agnostic manner, while the SCRMS-PIG provides a prioritized, dependency-aware roadmap to implement and govern those capabilities. These concepts form the basis for evaluating whether an entity has acted reasonably under legal, contractual and/or fiduciary scrutiny.

Together, these two (2) documents provide a structure to help ensure that an entity can credibly 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.

Due Diligence Under The SCRMS

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.

The SCRMS-PIG supports due diligence through Steps 1–26, which are intentionally sequenced to establish context, address dependencies and implement foundational capabilities. These steps produce a significant amount of defensible evidence. See Annex B – SCRMS Defensible Evidence for a list of possible artifacts.

Due Care Under The SCRMS

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.

The SCRMS-PIG supports due care through Steps 27–30, which are designed for executive and board-level engagement. These steps focus on governance oversight, recurring risk management, capability testing and strategic evolution of the SCR program.

Separation of Responsibilities

The SCRMS intentionally distinguishes execution from oversight:

- Management is responsible for designing, implementing and operating security, compliance and resilience capabilities; and
- Executives and the Board are responsible for oversight, risk acceptance and strategic direction.

This separation enables leadership to exercise due care without assuming operational or technical responsibilities, while maintaining documented accountability.

Concept	What It Means	Who Owns It
Due Diligence	Designing and implementing capabilities	Management
Due Care	Oversight, validation and evolution	Board & Executives

Critical Resource Enablement Path (CREP)

Security, compliance and resilience capability failures are rarely caused by missing controls, but by:

- Misaligned sequencing;
- Constrained resources; and/or
- Unmanaged dependencies.

The premise of the SCRMS-PIG is to build a viable project plan from the perspective of a prioritized listing of tasks to operationalize the SCRMS in the most efficient and effective manner possible. This helps establish an entity's **Critical Resource Enablement Path (CREP)**. CREP is a resource-flow governance mechanism that represents the sequence in which constrained resources must be enabled to prevent bottlenecks that undermine security, compliance and resilience outcomes. CREP ensures that foundational capabilities are established before dependent capabilities are introduced.

The CREP is an important concept since errors or misguided adventures with **People, Processes, Technologies, Data and/or Facilities (PPTDF)** earlier in SCRMS control implementation activities will have cascading effects, so the SCRMS-PIG is meant to provide a model for prioritizing efforts. For example, CREP can alter sequencing under budget constraints, supply chain issues and/or staffing shortages.

The SCRMS-PIG assists in clarifying an entity's CREP through breaking down SCRMS control implementation into thirty (30) major steps, which can then be translated into a viable project plan:

- Twenty-six (26) steps are focused on due diligence activities; and
- Four (4) steps are focused on due care activities.

NOTE: There is tremendous value from the cost of labor, business disruption and technology-related acquisition costs to void rework due to implementing capabilities where dependencies exist that result in cascading failures from misaligned PPTDF.

Theory of Constraints (TOC) Considerations

The SCRMS adopts the Theory of Constraints (TOC) because security, compliance and resilience capabilities are not optimized by maximizing individual control performance, but by identifying and managing the single most limiting constraint that prevents the entity from achieving reasonable, defensible outcomes.

In the context of the SCRMS, constraints most commonly manifest as deficiencies in **People, Processes, Technology, Data, or Facilities (PPTDF) and** unmanaged constraints at early stages create cascading failures in later SCRMS-PIG phases. CREP is the mechanism by which the SCRMS operationalizes TOC across PPTDF.

Constraint Type	Common SCRMS Example	Downstream Impact
People	No risk owner or insufficient staffing	Unmanaged POA&M items, delayed remediation
Processes	Immature change management	Unauthorized configurations and audit failures
Technologies	Lack of centralized logging	Lack of situational awareness
Data	Unknown data flows or classifications	Mishandling of sensitive / regulated data
Facilities	Inadequate physical security	Regulatory nonconformity

As with any process, an entity's cybersecurity program is always vulnerable due to the ability of the "weakest link" (e.g., person, part, supplier and/or process) to cause damage and adversely affect the overall cybersecurity program.

The **Theory of Constraints (TOC)** is a management paradigm that views any manageable system as being limited in achieving more of its goals by a very small number of constraints. There is always at least one constraint in a project/initiative and TOC utilizes a process to identify the constraint(s) and restructure the rest of the entity/processes around it.

TOC Management Focus

At the management level, TOC focuses on:

- Define business processes;
- Establish minimum quality requirements for people, processes and technologies;
- Establish, review and enforce contract requirements;
- Appropriately resource technical requirements; and
- Maintain situational awareness.

TOC Technical Focus

At the individual contributor level (e.g., analyst, engineer, technician, etc.), TOC focuses on:

- Define technical requirements;
- Identify and implement "industry recognized practices" to design, build and maintain systems, applications and services; and
- Provide metrics to management to maintain situational awareness.

Utilizing CREP To Operationalize SCRMS Capabilities

Applying TOC through the CREP enables an entity to demonstrate that resource allocation decisions were made rationally, based on identified constraints and documented dependencies. This provides objective evidence that management acted reasonably when prioritizing security, compliance and resilience investments.

This concept of the TOC/CREP is operationalized through the SCRMS-PIG in multiple scenarios:

- As an assessment readiness exercise;
- Prioritization decisions for a phased implementation plan; and
- As a method for introducing a new tool or capability into an existing environment.

Defining the entity's CREP fundamentally comes down to clearly distinguishing between facts and assumptions. This is the premise for compliance decision making:

- Facts are statements of truth, or statements thought to be true; and
- Assumptions are essentially gaps in knowledge or information that need to be confirmed or denied.

Examples include:

- An entity deploys a **Security Incident Event Manager (SIEM)** but lacks trained analysts and defined escalation procedures. Despite tooling investment, incident response effectiveness remains constrained by staffing and process maturity;
- An entity implements **Secure Baseline Configurations (SBC)**, but an immature change management process results in frequent unauthorized changes, negating the benefit of hardened baselines; and
- Risk acceptance decisions are made informally without documentation, resulting in an inability to demonstrate due care despite implemented controls.

Change Management CREP Considerations For The SCRMS

As an entity progresses through SCRMS controls, it is likely that new technologies and/or processes may be necessary. Technology change is inevitable and the entity may need to adjust the SCRMS-PIG for its specific needs and circumstances.

There are several factors that need to be considered when incorporating new technologies:

1. Define the necessary technology solution(s) by identifying the necessary PPTDF.
2. Identify suitable vendors based on the vendor's:
    a. Knowledge of the entity's statutory, regulatory and contractual obligations; and
    b. Ability to fill gaps related to those obligations.
3. Without exception, leverage the entity's change control processes to ensure the technology solutions are documented, reviewed and approved.
4. Leverage the SCRMS-PIG phases to identify where the entity will implement and operate the new technology solution to understand possible "cascading effects" of new technologies on other phases. For example:
    a. The entity will see a direct impact from a Security Information and Event Management (SIEM) tool during the following SCRMS-PIG phases:
        i. *Step 11. Network Security.*
        ii. *Step 14. Situational Awareness;*
        iii. *Step 15. Secure Baseline Configurations;*
        iv. *Step 16. Identity & Access Management (IAM); and*
        v. *Step 20. Attack Surface Management (Vulnerability Management);*
    b. The entity will see a direct impact from a security configuration / vulnerability scanning tool during the following SCRMS-PIG phases:
        i. *Step 12. Change Management;*
        ii. *Step 15. Secure Baseline Configurations; and*
        iii. *Step 20. Attack Surface Management (Vulnerability Management);*
5. Whenever multiple technology implementations overlap in a SCRMS-PIG phase, be aware of time and resource constraints.
    a. Add time allowances for the procurement, training, configuration and ongoing operation of the new technology solution; and
    b. Plan for the possibility that overlapping implementations may:
        i. Extend the time spent in a particular phase of the SCRMS-PIG; and
        ii. Increase labor-related expenses:
            1. Professional services from the vendor or managed IT service providers familiar with the solution; and/or
            2. Technical staff support from another internal team.
6. Integrate new technologies into Internal Audit (IA) practices to maintain the entity's information assurance capability and controls governance.
    a. This is the optimal time to develop performance measures (e.g., metrics) for assessing the continued effectiveness of the entity's newly implemented technology solutions.

BACKGROUND ON THE LOGIC USED IN THE SCRMS-PIG

For an explanation on the reasoning used for this model from a due diligence perspective:

- If an entity fails to establish context (e.g., facts & assumptions), the entire premise for compliance operations may be incorrect and that could lead the entity down the wrong path. From a due diligence perspective, establishing context for what constitutes "secure, compliant and resilient practices" should be a holistic endeavor. This partially includes defining all applicable laws, regulations and contractual obligations for cybersecurity and data protection, but it also includes a broader need to identify capabilities that need to exist to keep the entity security and compliant. This broad understanding enables the entity to implement proper governance practices (e.g., scope of compliance, stakeholders, supply chain protections, etc.).
- An entity can't legitimately assess changes, vulnerabilities, threats, etc. without first having a handle on risk management. Risk management is the key building block that other practices rely upon.
- There is a need to resource the **Security, Compliance & Resilience Plan (SCRP)**, but before it is possible to request resources it is necessary to gain situational awareness on dependencies for the funding justification:
  - Comprehensive inventories of:
    - **Technology Assets, Applications, Services and/or Data (TAASD)**;
    - **External Service Providers (ESP)**; and
    - **Cloud Service Providers (CSP)**.
  - Understanding of data flows (e.g., where sensitive and/or regulated data is stored, processed and/or transmitted).
  - Identification of critical **Technology Assets, Applications and/or Services (TAAS),** including business needs for **Recovery Time Objectives (RTOs)** and **Recovery Point Objectives (RPOs)**.
- With the context gained from the previous steps, including business continuity expectations for business critical TAASD, it is necessary to establish secure engineering criteria so that secure, compliant and resilient capabilities are implemented by design and by default throughout the **System Development Lifecycle (SDLC)**.
- Tied in closely with risk management and secure engineering is **Supply Chain Risk Management (SCRM)**, where it is very important to define requirements sooner rather than later in the SCRMS steps. The distributed nature of IT makes it very likely that nearly every entity has ESP and/or CSP that directly and indirectly affect the entity's ability to be secure, compliant and/or resilient. That requires the entity's requirements to flow down across its supply chain.
- The expectation is that entities implementing the SCRMS are large enough to have personnel assigned to cybersecurity roles. This is where defining operational security practices to maximize their impact is important.
- Without **Human Resource (HR)** support to enforce necessary behaviors, a cybersecurity program is more "security theater" than a functional cybersecurity program. This is where HR is involved in training employees through formal indoctrination for terms of employment and rules of behavior. This may involve retraining and potentially terminating employees that fail to adhere to those terms.
- Developing and implementing entity-wide data protection practices are crucial to limit logical and physical access to sensitive/regulated data (e.g., CHD, PII, ePHI, FCI, CUI, etc.). Technology is meant to follow practice, not the other way around where practices are modified to fit technology limitations. This means that technology should enable business practices to make the business more efficient, instead of technology solutions being implemented that hinder business practices.
- With the understanding of how business practices are meant to be supported, it should be possible to implement a segmented network architecture that can minimize the scope of compliance, while also supporting secure business practices. This includes on-premises and CSP instances.

- It is necessary to have **Change Management (CM)** matured to a state where it supports IT and business processes. CM is needed to legitimately alter other practices and the entity needs to be able to document its changes and track open issues in a POA&M (e.g., evidence of due care).
- From there, the assumption is that the entity will discover issues so incident response capability needs to exist.
- Situational awareness (e.g., event logging, centralized/automated log review, etc.) is next and needs to exist before secure configurations, since logs need to get sent somewhere. The entity needs to have this logging infrastructure in place before it get into secure configurations.
- **Secure Baseline Configurations (SBC)** and centralized management (e.g., STIGs, group policies, etc.) almost go hand-in-hand, but before the entity can centrally manage configurations, they need to be defined and standardized.
- Next, **Identity and Access Management (IAM)** needs to be locked down to ensure aspects of least privilege and **Role Based Access Control (RBAC)** are implemented. The reason IAM comes after secure configurations is due to troubleshooting - if the entity has a "gold standard" SBC to work with, it is easier to then assign permissions that will work with those builds. The alternative is its new configs break IAM/RBAC capabilities, which is bad and necessary to avoid.
- The entity realistically can't do vulnerability management without first having solid maintenance capabilities, so maintenance needs to be formalized with change control integrations. Maintenance needs to be tied to change management, which has a risk management component to it.
- The concept of vulnerability management is broad and is best summed up by the term **Attack Surface Management (ASM)** where the entity is doing what it can to minimize the ways an adversary can attack. This relies on maintenance practices and change management being in place and operating.
- From there, the remaining phases are relatively subjective - it really is. However, the "internal audit" function realistically needs to come last where control validation testing assesses how well controls are implemented. This can help serve as a pre-audit function.

For an explanation on the reasoning used for this model from a due care perspective:

- There is a need to have governance oversights to have situational awareness of the entity's ability to demonstrate conformity with its requirements.
- The concept of risk management is ongoing and never ending. There needs to be a capability to perform recurring risk assessments for internal capabilities, as well as across the supply chain. From a supply chain perspective, it is very important to track and assess changes, since those changes may be unacceptable based on the initial risk assessment.
- Testing capabilities is important to avoid incorrect assumptions. This primarily focuses on testing and validating risk management and **Business Continuity / Disaster Recovery (BC/DR)** capabilities.
- At the end of the day, the responsibility for evolving capabilities rests with an entity's executive leadership. The due care components involve providing recurring status reports (e.g., quarterly business reviews) with sufficient information for strategic decision making to occur.

SCRMS Due Diligence Steps

The SCRMS-PIG breaks down SCRMS control implementation into thirty (30) major steps, where twenty-six (26) steps are focused on due diligence activities.

Step 1 - Establish Context For Security, Compliance & Resilience (SCR) Operations

If the entity fails to establish context (e.g., facts & assumptions), the entity's entire premise for compliance operations may be incorrect and that could lead it down the wrong path. From a due diligence perspective, establishing context for security, compliance & resilience capabilities should be a holistic endeavor that starts with understanding the mission of the entity and how its business operations function. The reason for this is it is better to have a complete understanding of all requirements at the beginning to avoid reworking in the future, which sacrifices both time and resources.

This step has seven (7) sub-component steps:

a) Define the entity's mission to establish the business context for necessary SCR capabilities.
b) Establish a **Security, Compliance & Resilience Program (SCRP)**, including enforcement & resourcing authority.
c) Define **Minimum Compliance Requirements (MCR).** Identify the entity's applicable statutory, regulatory and contractual obligations for cybersecurity and data protection.
d) Define preliminary **Discretionary Secure Requirements (DSR)**. Identify reasonable security and resilience expectations, based on applicable threats and risks (e.g., risk & threat catalogs).
e) Define the preliminary **Living Control Set (LCS)** for the entity, based on DSR and MCR. This is the **Minimum Security Requirements (MSR)** baseline.
f) Define the scope of the SCRP, based on the LCS and applicable **People, Processes, Technology, Data & Facilities (PPTDF)**.
g) Define target maturity criteria at the domain or control level for the LCS.

Step 2 – Implement Centralized Governance Practices

With an understanding of what the entity's mission and business objectives are, it is possible to implement appropriate governance practices.

This step has four (4) sub-component steps:

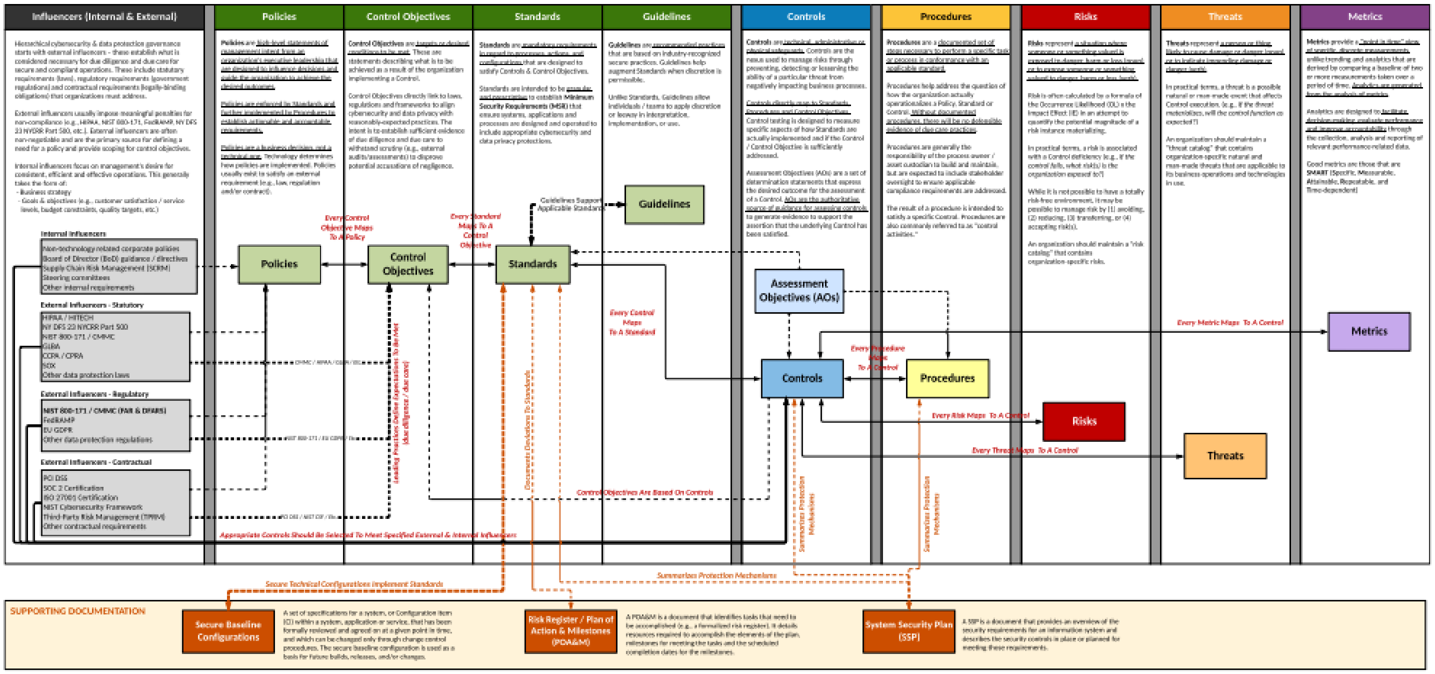
a) From a centralized authority, develop, implement and maintain policies and standards to address SCRP needs, based on the LCS.*
b) Provide the capability to manage exception requests to published standards.
c) Provide a commitment to continuously improve security, compliance & resilience capabilities.
d) Identify stakeholders and assign control ownership from the LCS to applicable stakeholders. Stakeholders develop and maintain **Standardized Operating Procedures (SOP)** to implement controls.

* 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: [3]

- Policies;
- Control objectives;

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

- Standards;
- Guidelines;
- Controls;
- Assessment Objectives (AOs);
- Risks;
- Threats;
- Procedures; and
- Metrics.


Influencers (Internal & External)
Policies
Control Objectives
Standards
Guidelines
Controls
Procedures
Risks
Threats
Metrics
Internal Influencers
Non-technology related corporate policies
Board of Director (BoD) guidance / directives
Supply Chain Risk Management (SCRM)
Steering committees
Other internal requirements
External Influencers - Statutory
HIPAA / HITECH
NY DFS 23 NYCRR Part 500
NIST 800-171 / CMMC
GLBA
CCPA / CPRA
SOX
Other data protection laws
External Influencers - Regulatory
NIST 800-171 / CMMC (FAR & DFARS)
FedRAMP
EU GDPR
Other data protection regulations
External Influencers - Contractual
PCI DSS
SOC 2 Certification
ISO 27001 Certification
NIST Cybersecurity Framework
Third-Party Risk Management (TPRM)
Other contractual requirements
Every Control Objective Maps To A Policy
Every Standard Maps To A Control Objective
Guidelines Support Applicable Standards
Every Control Maps To A Standard
Assessment Objectives (AOs)
Every Procedure Maps To A Control
Every Metric Maps To A Control
Every Risk Maps To A Control
Every Threat Maps To A Control
Leading Practices Define Expectations To Be Met (due diligence / due care)
Documents Deviations To Standards
Control Objectives Are Based On Controls
Summarizes Protection Mechanisms
Appropriate Controls Should Be Selected To Meet Specified External & Internal Influencers
Secure Technical Configurations Implement Standards
SUPPORTING DOCUMENTATION
Secure Baseline Configurations
Risk Register / Plan of Action & Milestones (POA&M)
System Security Plan (SSP)

A set of specifications for a system, or Configuration Item (CI) within a system, application or service, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The secure baseline configuration is used as a basis for future builds, releases, and/or changes.

A POA&M is a document that identifies tasks that need to be accomplished (e.g., a formalized risk register). It details resources required to accomplish the elements of the plan, milestones for meeting the tasks and the scheduled completion dates for the milestones.

A SSP is a document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

STEP 3 - ALIGN RISK MANAGEMENT PRACTICES ACROSS THE ENTITY

Risk management is the key building block that other practices rely upon. It is infeasible to govern changes and/or assess vulnerabilities, threats, etc. without first having established risk management practices. Risk management practices establish thresholds for acceptable risk for both internal and external stakeholders.

Cybersecurity does not exist in isolation and it is crucial for cybersecurity and data protection-related risk management to be subordinate to the entity's overall **Enterprise Risk Management (ERM)** practices.

This step has six (6) sub-component steps:

a) Develop & implement an entity-wide **Risk Management Program (RMP)** for SCRP operations to identify, assess and remediate risk that is tied into ERM practices.
b) Define entity-specific risk appetite, risk threshold and risk tolerance criteria.
c) Define materiality for the entity. Utilize that criteria to define material controls, material incidents, material threats and material risks.
d) Define a risk assessment methodology that is appropriate for the entity's SCRP needs to identify, categorize and assess risks.
e) Define stakeholder requirements for risk remediation actions to remediate risks to an acceptable level.
f) Develop a centralized risk register, or **Plan of Action & Milestones (POA&M)**, to provide situational awareness of risks and govern remediation activities.

Step 4 - Gain Clarity On The Entity's PPTDF

Operationalizing security, compliance & resilience practices will be misguided without first understanding the entity's **Technology Assets, Applications, Services and/or Data (TAASD)**, including criticality decisions. That understanding has cascading implications.

This step has seven (7) sub-component steps:

a) Create and maintain a detailed inventory for all TAASD.
b) Create and maintain a detailed inventory for all **External Service Providers (ESP)** and **Cloud Service Providers (CSP)**.
c) Create and maintain a detailed inventory for all sensitive and/or regulated data, including geolocation.
d) Create detailed network diagrams that cover all **Technology Assets, Applications and/or Services (TAAS)**, including TAAS maintained by ESP and/or CSP.
e) Create **Data Flow Diagrams (DFD)** that shows how sensitive and/or regulated data flows across the entity's TAAS, including contractor flow-down.
f) Identify critical TAAS, including ESP and CSP.
g) Based on the entity's mission and business operations, define preliminary **Recovery Time Objectives (RTOs)** and **Recovery Point Objectives (RPOs)** to provide context to asset criticality.

Step 5 - Resource The SCRP

Resourcing the SCRP involves planning (e.g., business plan, budget request, prioritized road map, etc.). This is a function between the **Chief Information Security Officer (CISO)** and a **Program Management Office (PMO)**, or similar function, to build a prioritized roadmap and obtain stakeholder buy-in.

This step has two (2) sub-component steps:

a) Develop & implement a resource plan (e.g., business plan, budget, road map, etc.) to operationalize the entity's SCRP (e.g., necessary PPTDF components).
b) Prioritize stakeholder objectives based on the resource plan for PPTDF.

Step 6 - Establish Criteria To Be Secure, Compliant & Resilient

Assumptions need to be avoided and when it comes to security, compliance & resilience capabilities, which comes down to defining "secure practices" that can be applied across the **System Development Lifecycle (SDLC)**. This includes planning for performance and capabilities to ensure the resilience of business functions. It also includes the expectation to provide assurance through pre-production testing activities.

This step has six (6) sub-component steps:

a) Secure engineering principles are defined to ensure security, compliance & resilience capabilities are implemented by default and by design.
b) Stakeholders govern security, compliance & resilience requirements across the System Development Lifecycle (SDLC).
c) Security, compliance & resilience capabilities are implemented by default and by design in product management processes (e.g., updates, features, etc.).
d) Implement a capacity and performance management capability to support resilience requirements.
e) Implement an **Information Assurance Program (IAP)** to ensure secure, compliant & resilient capabilities are included by default and by design.

f) Implement **Risk Treatment Plans (RTP)** that include viable compensating controls when primary controls cannot be implemented or are deficient.

STEP 7 - ESTABLISH CAPABILITIES TO SECURE THE SUPPLY CHAIN

The ability to secure the supply chain is much larger than just the cybersecurity team. This likely will involve procurement, data privacy, contracts management and the **Chief Operations Officer (COO)**, since changes to the supply chain can have direct effects on business operations and that requires involvement from the COO, or a similar role, to avoid disruptions.

This step has five (5) sub-component steps:

a) Develop a **Cybersecurity Supply Chain Risk Management (C-SCRM)** Plan that is applicable across the entity.
b) Develop and implement acquisition strategies, contract tools and procurement methods to operationalize the C-SCRM Plan.
c) Enforce C-SCRM requirements across the supply chain through contracts and flow-down requirements.
d) Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.
e) Create a **Responsible, Accountable, Supportive, Consulted & Informed (RASCI)** matrix to eliminate assumptions with ESP.

STEP 8 – CYBERSECURITY OPERATIONS

This involves implementing empowering cybersecurity and data protection personnel to enforce secure, compliant and resilient practices. POA&M deficiencies.

STEP 9 – HUMAN RESOURCES (HR) PRACTICES

This involves working with the **Human Resources (HR)** department to ensure personnel security requirements are integrated into HR operations. POA&M deficiencies.

STEP 10 – DATA CLASSIFICATION & HANDLING

This involves defining and implementing processes to securely handle data wherever it is stored, processed and/or transmitted. Limit logical and physical access to sensitive and/or regulated data. POA&M deficiencies.

STEP 11 – NETWORK SECURITY

This involves developing and implementing a segmented network architecture and industry-recognized secure practices for network security. POA&M deficiencies.

STEP 12 – CHANGE MANAGEMENT

This involves developing and implementing change control processes, including a **Change Control Board (CCB)**. POA&M deficiencies.

STEP 13 – INCIDENT RESPONSE OPERATIONS

This involves developing and implementing incident response capabilities to detect, respond and recover from incidents. POA&M deficiencies.

STEP 14 – SITUATIONAL AWARENESS THROUGH CONTINUOUS MONITORING

This involves developing and implementing situational awareness capabilities through threat intelligence, log collection and analysis (e.g., SIEM). POA&M deficiencies.

STEP 15 – SECURE BASELINE CONFIGURATIONS (SBC)

This involves developing and implementing **Secure Baseline Configurations (SBC)** (e.g., hardening standards) for all technology platforms and enforcing secure configurations (e.g., Directory Services, Active Directory, Intune, etc.). POA&M deficiencies.

STEP 16 – IDENTITY & ACCESS MANAGEMENT (IAM)

This involves developing and implementing **Identity & Access Management (IAM)** capabilities to address "least privilege" and **Role-Based Access Control (RBAC)**. POA&M deficiencies.

STEP 17 – IT ASSET MANAGEMENT (ITAM)

This involves developing and implementing **Information Technology Asset Management (ITAM)** practices, including **Endpoint Device Management (EDM)**. POA&M deficiencies.

STEP 18 – EMBEDDED TECHNOLOGIES

This involves developing and implementing embedded technology governance practices for **Operational Technology (OT)** and **Internet of Things (IoT)** assets. POA&M deficiencies.

STEP 19 – PROACTIVE MAINTENANCE

This involves developing and implementing proactive maintenance practices. POA&M deficiencies.

STEP 20 – ATTACK SURFACE MANAGEMENT (ASM)

This involves developing and implementing **Attack Surface Management (ASM)** practices. POA&M deficiencies.

STEP 21 – ARTIFICIAL INTELLIGENCE GOVERNANCE (AIG)

This involves developing and implementing **Artificial Intelligence & Autonomous Technologies (AAT)** governance practices. POA&M deficiencies.

STEP 22 – CONTINUITY OF OPERATIONS PLAN (COOP)

This involves developing and implementing **Business Continuity & Disaster Recovery (BC/DR)** capabilities. POA&M deficiencies.

STEP 23 – DATA PRIVACY PROGRAM

This involves developing and implementing a data privacy program. POA&M deficiencies.

STEP 24 – PHYSICAL & ENVIRONMENTAL SECURITY

This involves developing and implementing physical and environmental security capabilities. POA&M deficiencies.

STEP 25 – SECURITY-MINDED WORKFORCE

This involves developing and implementing a security-minded workforce through security, compliance & resilience training & awareness. POA&M deficiencies.

STEP 26 – THREAT INTELLIGENCE

This involves developing and implementing a **Threat Intelligence Program (TIP)**. POA&M deficiencies.

SCRMS Due Care Focus

The SCRMS-PIG breaks down SCRMS control implementation into thirty (30) major steps, where four (4) steps are focused on due care activities.

Step 27 – Governance Oversight

This involves providing oversight of **Security, Compliance & Resilience Program (SCRP)** controls, including deficiencies and remediation activities.

Due Care Purpose:

- Provide stakeholders with assurance that controls are implemented and operating as designed; and
- Transparency on known deficiencies, including planned remediation actions.

Evidence the Board Should Expect:

- Results from conformity assessments (internal or third-party); and
- Status of open **Plan of Action & Milestone (POA&M)** items.

Board's Role In This Step:

- Challenge assumptions;
- Confirm capability implementation priorities align with business risk;
- Ensure unresolved risks are consciously accepted; and
- Challenge assumptions.

Reasonable Board Questions:

- *Are controls actually implemented?*
- *Where are we knowingly deficient?*
- *Are remediation efforts tracked and funded?*

Red Flags:

- "Everything is green" with no documented exceptions; and
- No remediation actions for known deficiencies.

Step 28 – Risk Management

This involves managing changes that affect the entity's security, compliance & resilience, including the supply chain.

Due Care Purpose:

- Provide a "reality check" to stakeholders that cyber risk is never static; and
- Maintain situational awareness of supply chains, technology, threats and compliance obligations, since those are dynamic areas that change often.

Evidence the Board Should Expect:

- Updated risk register;
- Risk acceptance decisions;
- Supply chain risk summaries;
- Number of material risks;
- Trend of unresolved risks;
- Risk acceptance vs remediation ratio;

- Time-to-remediate critical findings; and
- Testing failures and lessons learned.

Board's Role In This Step:

- Confirm remediation priorities align with business risk;
- Ensure unresolved risks are properly managed through remediation or acceptance; and
- Challenge assumptions.

Reasonable Board Questions:

- *Has our risk profile changed since last quarter?*
- *Have suppliers, cloud providers, or partners introduced new risk?*
- *Are accepted risks still acceptable?*

Red Flags:

- No remediation action on material risks; and
- Active certification(s) where there are unresolved POA&M entries that are in-scope for the certification.

STEP 29 – CAPABILITY TESTING

This involves test processes to ensure they are secure, compliant and resilient.

Due Care Purpose:

- Validate assumptions;
- Detect false confidence; and
- Prove resilience under stress.

Evidence the Board Should Expect:

- **Root Cause Analysis (RCA)** results from recent incidents; and
- Testing results for:
  - Incident response capabilities; and
  - Business response capabilities.

Board's Role In This Step:

- Determine resilience capabilities support business needs; and
- Challenge assumptions.

Reasonable Board Questions:

- *What failed in testing?*
- *What assumptions were invalid?*
- *What was corrected as a result?*

Red Flags:

- No RCA findings following significant incidents; and
- Testing that produces no findings.

STEP 30 – EVOLVING CAPABILITIES

This involves reporting the status of the SCRP to a governing body (e.g., quarterly business reviews to a steering committee).

Due Care Purpose:

- Redefining “reasonable security, compliance & resilience” capabilities as conditions changes over time;
- Provide situational awareness through:
  - **Quarterly Business Reviews (QBR)**;
  - Event-driven reviews (e.g., incidents, **Mergers, Acquisitions and Divestitures (MA&D)** activities, compliance changes, etc.); and/or
  - Annual business planning.

Evidence the Board Should Expect:

- Clarification on evolving statutory, regulatory and/or contractual requirements;
- Prioritized plans (including resource requirements) to evolve current capabilities to address evolving requirements.

Board’s Role In This Step:

- Determine the entity’s necessary:
  - Strategic adjustments;
  - Capability maturation; and
  - Risk posture adjustments; and
- Challenge assumptions.

Reasonable Board Questions:

- *How do the changes to [law / regulation / framework] affect us?*
- *What are the legal, financial and reputational damages associated with non-compliance?*

Red Flags:

- “Everything is fine” where no improvements are needed; and
- No open remediation actions exist for known deficiencies.

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.

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.[4]

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 organizations 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.

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.

[4] *Security, Compliance & Resilience Conformity Assessment Program (SCR CAP) -* https://securecontrolsframework.com/training-certifications/scf-certifications/scf-conformity-assessment-program-cap/

APPENDICES

APPENDIX A – SCRMS CONTROLS PRIORITIZATION

The following table contains the SCF controls from the SCRMS and displays it in a prioritized format, based on the SCRMS-PIG.

NOTE: Controls with a score of 10 in the Relative Control Weighting column should be considered material controls, where there is no reasonable compensating control that can be used to make up for a deficiency associated with that control.

SCRMS-PIG Step	SCF #	SCF Control	Relative Control Weighting	PPTDF Applicability	Conformity Validation Cadence (CVC)	Evidence Request List (ERL) #
1a	GOV-08	Defining Business Context & Mission	5	Process	Annual	E-PRM-01
1b	GOV-01	Cybersecurity & Data Protection Governance Program	10	Process	Annual	E-GOV-01 E-GOV-02
	GOV-01.1	Steering Committee & Program Oversight	7	Process	Annual	E-GOV-03 E-PRM-06
	GOV-04	Assigned Cybersecurity & Data Protection Responsibilities	10	People	Annual	E-HRS-01 E-HRS-05 E-HRS-06 E-HRS-07 E-HRS-08 E-HRS-09 E-HRS-10 E-HRS-13 E-HRS-15
	GOV-04.1	Stakeholder Accountability Structure	8	Process	Annual	E-HRS-15
1c	CPL-01	Statutory, Regulatory & Contractual Compliance	10	Process	Semi-Annual	E-CPL-01 E-GOV-10
	GOV-15.1	Select Controls	8	Process	Annual	
1d	GOV-15.1	Select Controls	8	Process	Annual	
	RSK-03.1	Risk Catalog	5	Process	Annual	E-RSK-09
	THR-09	Threat Catalog	5	Process	Annual	E-THR-06
1e	GOV-15	Operationalizing Cybersecurity & Data Protection Practices	9	Process	Annual	E-GOV-19
	GOV-15.1	Select Controls	8	Process	Annual	
1f	CPL-01.2	Compliance Scope	10	Process	Semi-Annual	E-AST-02 E-CPL-02 E-GOV-10
1g	PRM-01.2	Targeted Capability Maturity Levels	5	Process	Annual	E-PRM-04
2a	GOV-02	Publishing Cybersecurity & Data Protection Documentation	10	Process	Annual	E-GOV-08 E-GOV-09 E-GOV-11
2b	GOV-02.1	Exception Management	8	Process	Annual	E-GOV-18
2c	GOV-01.2	Status Reporting To Governing Body	5	Process	Annual	E-CPL-05 E-CPL-09 E-GOV-03 E-GOV-04 E-GOV-05 E-GOV-06 E-GOV-07 E-GOV-13
	GOV-01.3	Commitment To Continual Improvements	7	Process	Annual	
2d	AST-01.2	Stakeholder Identification & Involvement	5	Process	Annual	E-CPL-03
	GOV-15.2	Implement Controls	9	Process	Annual	
	OPS-01.1	Standardized Operating Procedures (SOP)	9	Process	Annual	E-GOV-11
3a	RSK-01	Risk Management Program	10	Process	Annual	E-RSK-01

3b	RSK-01.3	Risk Tolerance	9	Process	Annual	E-RSK-06
	RSK-01.4	Risk Threshold	9	Process	Annual	E-RSK-07
	RSK-01.5	Risk Appetite	9	Process	Annual	E-RSK-08
3c	GOV-15.1	Select Controls	8	Process	Annual	
	GOV-16	Materiality Determination	7	Process	Annual	E-GOV-14
	GOV-16.1	Material Risks	7	Process	Annual	E-GOV-15
	GOV-16.2	Material Threats	7	Process	Annual	E-GOV-16
3d	RSK-01.1	Risk Framing	9	Process	Annual	E-RSK-01 E-RSK-06 E-RSK-07 E-RSK-08
	RSK-03	Risk Identification	9	Process	Annual	E-RSK-04
	RSK-04	Risk Assessment	10	Process	Annual	E-RSK-04
	RSK-04.1	Risk Register	10	Process	Semi-Annual	E-RSK-03
	RSK-04.2	Risk Assessment Methodology	8	Process	Annual	
	RSK-05	Risk Ranking	9	Process	Annual	E-RSK-04
3e	IAO-05	Plan of Action & Milestones (POA&M)	9	Process	Annual	E-RSK-03
	RSK-04.1	Risk Register	10	Process	Semi-Annual	E-RSK-03
	RSK-06	Risk Remediation	10	Process	Semi-Annual	E-RSK-03
4a	AST-02	Asset Inventories	10	Process	Annual	E-AST-04 E-AST-05 E-AST-07 E-AST-28
4b	TPM-01.1	Third-Party Inventories	8	Process	Annual	E-AST-06 E-DCH-06
4c	CLD-09	Geolocation Requirements for Processing, Storage and Service Locations	10	Process	Semi-Annual	E-AST-06 E-AST-23 E-DCH-15
	DCH-06.2	Sensitive Data Inventories	9	Data	Annual	E-AST-08
	DCH-19	Geographic Location of Data	9	Data	Annual	E-AST-23
	DCH-24	Information Location	10	Data	Annual	E-AST-23
	PRI-05.5	Inventory of Personal Data (PD)	8	Data	Annual	E-AST-08
	TPM-04.4	Third-Party Processing, Storage and Service Locations	10	Process	Annual	E-AST-23
4d	AST-04	Network Diagrams & Data Flow Diagrams (DFDs)	10	Process	Annual	E-DCH-03 E-DCH-04 E-DCH-05
4e	AST-02.8	Data Action Mapping	9	Process	Semi-Annual	E-DCH-05
	AST-04	Network Diagrams & Data Flow Diagrams (DFDs)	10	Process	Annual	E-DCH-03 E-DCH-04 E-DCH-05
4f	BCD-01.4	Recovery Time / Point Objectives (RTO / RPO)	5	Process	Annual	E-BCM-02 E-BCM-03
	BCD-02	Identify Critical Assets	9	Process	Annual	E-BCM-08
	TPM-02	Third-Party Criticality Assessments	9	Process	Annual	E-TPM-02
5a	PRM-01	Cybersecurity & Data Protection Portfolio Management	8	Process	Annual	E-PRM-02
	PRM-01.1	Strategic Plan & Objectives	5	Process	Annual	E-PRM-01
	PRM-03	Allocation of Resources	8	Process	Annual	E-PRM-01 E-PRM-02
5b	PRM-01	Cybersecurity & Data Protection Portfolio Management	8	Process	Annual	E-PRM-02
	PRM-01.1	Strategic Plan & Objectives	5	Process	Annual	E-PRM-01
	PRM-03	Allocation of Resources	8	Process	Annual	E-PRM-01 E-PRM-02
	PRM-04	Cybersecurity & Data Protection In Project Management	10	Process	Annual	E-PRM-03 E-PRM-05
	PRM-05	Cybersecurity & Data Protection Requirements Definition	9	Process	Annual	E-PRM-03 E-PRM-05

6a	SEA-01	Secure Engineering Principles	10	Process	Annual	E-TDA-01 E-TDA-02 E-TDA-04 E-TDA-08 E-TDA-09
	SEA-01.2	Achieving Resilience Requirements	4	Process	Annual	E-BCM-01 E-GOV-10 E-GOV-12
	SEA-01.3	Resilience Capabilities	5	Technology	Annual	
	SEA-02	Alignment With Enterprise Architecture	9	Process	Annual	E-TDA-04 E-TDA-09
	SEA-02.3	Technical Debt Reviews	9	Process	Annual	
	SEA-03	Defense-In-Depth (DiD) Architecture	10	Technology	Annual	E-TDA-04 E-TDA-09
	SEA-20	Clock Synchronization	9	Technology	Annual	
6b	PRM-05	Cybersecurity & Data Protection Requirements Definition	9	Process	Annual	E-PRM-03 E-PRM-05
	PRM-07	Secure Development Life Cycle (SDLC) Management	10	Process	Annual	E-PRM-03
6c	TDA-01	Technology Development & Acquisition	10	Process	Annual	E-TDA-01 E-TDA-02 E-TDA-08 E-TDA-17
	TDA-01.1	Product Management	10	Process	Annual	E-CPL-06 E-TDA-05 E-TDA-06 E-TDA-07 E-TDA-15 E-TDA-17
	TDA-01.4	DevSecOps	6	Process	Annual	
	TDA-02	Minimum Viable Product (MVP) Security Requirements	9	Process	Annual	E-TDA-06
	TDA-02.10	Product Testing & Reviews	9	Process	Quarterly	
	TDA-02.3	Development Methods, Techniques & Processes	5	Process	Annual	E-TDA-04
	TDA-04.2	Software Bill of Materials (SBOM)	9	Process	Annual	E-TDA-12
	TDA-05	Developer Architecture & Design	8	Process	Annual	E-TDA-04
	TDA-06	Secure Software Development Practices (SSDP)	10	Process	Annual	E-TDA-08 E-TDA-11
	TDA-06.1	Criticality Analysis	9	Process	Annual	E-BCM-08 E-CHG-01 E-TPM-02
	TDA-06.2	Threat Modeling	7	Process	Annual	E-TDA-03 E-TDA-10 E-THR-05
	TDA-06.5	Software Design Review	10	Process	Annual	E-TDA-05
	TDA-07	Secure Development Environments	9	Process	Annual	
	TDA-20	Access to Program Source Code	9	Process	Annual	
6d	CAP-01	Capacity & Performance Management	8	Process	Annual	E-CAP-01
	CAP-03	Capacity Planning	8	Process	Annual	E-CAP-01
	CAP-05	Elastic Expansion	5	Technology	Annual	E-CAP-04
6e	GOV-15.3	Assess Controls	8	Process	Annual	
	GOV-15.4	Authorize Technology Assets, Applications and/or Services (TAAS)	8	Process	Annual	
	IAO-01	Information Assurance (IA) Operations	10	Process	Annual	E-IAO-01
	IAO-02	Assessments	10	Process	Semi-Annual	E-IAO-03 E-IAO-04
	IAO-02.4	Security Assessment Report (SAR)	7	Process	Annual	E-IAO-01 E-IAO-03 E-IAO-05
	IAO-03	System Security & Privacy Plan (SSPP)	7	Process	Annual	E-TDA-14

	IAO-04	Threat Analysis & Flaw Remediation During Development	10	Process	Annual	
	IAO-05	Plan of Action & Milestones (POA&M)	9	Process	Annual	E-RSK-03
	IAO-06	Technical Verification	8	Process	Annual	
6f	RSK-06.1	Risk Response	9	Process	Semi-Annual	E-RSK-03
	RSK-06.2	Compensating Countermeasures	9	Process	Annual	E-GOV-20 E-RSK-03
	RSK-06.4	Risk Treatment Plan	9	Process	Semi-Annual	E-RSK-14
7a	RSK-09	Supply Chain Risk Management (SCRM) Plan	10	Process	Annual	E-RSK-02
	TPM-03	Supply Chain Risk Management (SCRM)	9	Process	Annual	E-RSK-02
7b	TPM-01	Third-Party Management	10	Process	Annual	E-TPM-03 E-TPM-06
	TPM-03	Supply Chain Risk Management (SCRM)	9	Process	Annual	E-RSK-02
	TPM-04	Third-Party Services	10	Process	Annual	E-CPL-06
7c	TPM-05	Third-Party Contract Requirements	10	Process	Annual	E-RSK-02 E-TPM-01 E-TPM-03 E-TPM-06 E-TPM-07
	TPM-05.2	Contract Flow-Down Requirements	9	Process	Annual	E-RSK-02
	TPM-05.7	Break Clauses	9	Process	Annual	E-TPM-05
7d	RSK-09.1	Supply Chain Risk Assessment	9	Process	Annual	E-RSK-05
	TPM-04.1	Third-Party Risk Assessments & Approvals	9	Process	Annual	E-TPM-01 E-TPM-02 E-TPM-03
7e	TPM-05.4	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	8	Process	Annual	E-CPL-03
8	OPS-01	Operations Security	8	Process	Annual	E-HRS-01 E-HRS-03 E-HRS-04 E-HRS-13 E-HRS-15 E-HRS-27
	OPS-02	Security Concept Of Operations (CONOPS)	9	Process	Annual	
	OPS-03	Service Delivery (Business Process Support)	7	Process	Annual	E-TPM-04
9	HRS-01	Human Resources Security Management	10	Process	Annual	E-HRS-01 E-HRS-15 E-HRS-27
	HRS-03	Defined Roles & Responsibilities	10	People	Annual	E-HRS-01 E-HRS-02 E-HRS-03 E-HRS-04 E-HRS-11 E-HRS-13 E-HRS-18 E-HRS-22 E-HRS-28
	HRS-03.2	Competency Requirements for Security-Related Positions	9	People	Annual	E-HRS-21 E-HRS-23
	HRS-04	Personnel Screening	10	People	Annual	E-HRS-17 E-HRS-21
	HRS-04.1	Roles With Special Protection Measures	9	People	Annual	E-HRS-17 E-HRS-21
	HRS-05	Terms of Employment	10	People	Annual	E-HRS-16 E-HRS-22
	HRS-05.1	Rules of Behavior	10	People	Annual	E-HRS-22
	HRS-05.7	Policy Familiarization & Acknowledgement	8	People	Annual	E-HRS-18 E-SAT-02 E-SAT-04
	HRS-07	Personnel Sanctions	9	People	Annual	E-HRS-27 E-HRS-29

	HRS-07.1	Workplace Investigations	8	People	Annual	
	HRS-08	Personnel Transfer	9	People	Annual	E-HRS-29
	HRS-09	Personnel Termination	9	People	Annual	E-HRS-19 E-HRS-29
	HRS-10	Third-Party Personnel	10	People	Annual	E-HRS-16 E-HRS-18 E-HRS-22
	HRS-13	Identify Critical Skills & Gaps	5	Process	Annual	E-HRS-23 E-HRS-24
	HRS-14	Identifying Authorized Work Locations	8	Process	Annual	
10	DCH-01	Data Protection	10	Data	Annual	E-CRY-01
	DCH-01.2	Sensitive / Regulated Data Protection	9	Data	Annual	E-CRY-01 E-DCH-02 E-DCH-09
	DCH-01.4	Defining Access Authorizations for Sensitive / Regulated Data	9	Process	Annual	E-DCH-02 E-DCH-08
	DCH-02	Data & Asset Classification	10	Data	Semi-Annual	E-DCH-01 E-DCH-02
	DCH-13	Use of External Technology Assets, Applications and/or Services (TAAS)	9	Technology	Annual	
	DCH-13.3	Protecting Sensitive / Regulated Data on External Technology Assets, Applications and/or Services (TAAS)	10	Data	Semi-Annual	
	DCH-17	Ad-Hoc Transfers	8	Data	Annual	
	DCH-18	Media & Data Retention	8	Data	Semi-Annual	E-AST-11
	DCH-19	Geographic Location of Data	9	Data	Annual	E-AST-23
	DCH-21	Information Disposal	10	Data	Annual	
	DCH-24	Information Location	10	Data	Annual	E-AST-23
	DCH-25	Transfer of Sensitive and/or Regulated Data	10	Data	Annual	
11	CLD-01	Cloud Services	10	Process	Annual	E-AST-06
	CLD-02	Cloud Security Architecture	8	Process	Annual	E-TDA-09
	CLD-09	Geolocation Requirements for Processing, Storage and Service Locations	10	Process	Semi-Annual	E-AST-06 E-AST-23 E-DCH-15
	CLD-10	Sensitive Data In Public Cloud Providers	6	Data	Annual	E-AST-08
	NET-01	Network Security Controls (NSC)	10	Technology	Annual	E-NET-04
	NET-02	Layered Network Defenses	9	Technology	Annual	E-DCH-03 E-DCH-04 E-DCH-05
	NET-02.2	Guest Networks	6	Technology	Annual	
	NET-03	Boundary Protection	10	Technology	Annual	E-NET-08 E-NET-09
	NET-04	Data Flow Enforcement – Access Control Lists (ACLs)	10	Technology	Annual	E-AST-12 E-AST-19 E-NET-06 E-NET-07 E-NET-10
	NET-04.1	Deny Traffic by Default & Allow Traffic by Exception	10	Technology	Annual	E-AST-12 E-AST-19 E-NET-07 E-NET-10
	NET-10	Domain Name Service (DNS) Resolution	10	Technology	Annual	
	NET-12	Safeguarding Data Over Open Networks	8	Technology	Annual	
	NET-12.2	End-User Messaging Technologies	9	Technology	Annual	
	NET-14	Remote Access	10	Technology	Annual	E-NET-03 E-IAM-14
	NET-14.5	Work From Anywhere (WFA) - Telecommuting Security	10	Process	Annual	E-NET-03 E-IAM-14
	NET-14.7	Endpoint Security Validation	6	Technology	Quarterly	
	NET-15	Wireless Networking	9	Technology	Annual	
	NET-18	DNS & Content Filtering	9	Technology	Annual	E-NET-01
	WEB-01	Web Security	8	Process	Annual	

	WEB-10	Secure Web Traffic	9	Technology	Annual	
12	CHG-01	Change Management Program	10	Process	Annual	E-CHG-02
	CHG-02	Configuration Change Control	8	Process	Annual	E-CHG-02 E-CHG-05
	CHG-02.1	Prohibition Of Changes	10	Process	Annual	E-CHG-02
	CHG-03	Security Impact Analysis for Changes	9	Process	Annual	E-CHG-04
13	IRO-01	Incident Response Operations	9	Process	Annual	E-IRO-01
	IRO-02	Incident Handling	10	Process	Annual	E-IRO-03
	IRO-03	Indicators of Compromise (IOC)	8	Process	Semi-Annual	E-IRO-02
	IRO-04	Incident Response Plan (IRP)	9	Process	Annual	E-IRO-01
	IRO-07	Integrated Security Incident Response Team (ISIRT)	9	Process	Annual	E-IRO-01 E-IRO-09
	IRO-10	Incident Stakeholder Reporting	9	Process	Annual	E-IRO-01 E-IRO-11 E-IRO-13
	IRO-13	Root Cause Analysis (RCA) & Lessons Learned	8	Process	Annual	E-IRO-08
14	MON-01	Continuous Monitoring	10	Technology	Annual	E-MON-01 E-MON-06 E-MON-07
	MON-01.2	Automated Tools for Real-Time Analysis	9	Technology	Annual	E-MON-01 E-MON-05
	MON-01.4	System Generated Alerts	7	Technology	Semi-Annual	E-END-03 E-MON-01 E-MON-06 E-MON-07
	MON-01.8	Security Event Monitoring	10	Process	Annual	E-MON-01 E-MON-02 E-MON-05
	MON-03	Content of Event Logs	10	Technology	Annual	E-AST-01 E-CPL-01
	MON-11.3	Monitoring for Indicators of Compromise (IOC)	5	Technology	Quarterly	E-IRO-02 E-MON-07
	MON-16	Anomalous Behavior	10	Technology	Semi-Annual	E-IRO-02 E-MON-07
	THR-03	Threat Intelligence Feeds	8	Process	Annual	E-THR-03
15	CFG-01	Configuration Management Program	9	Process	Annual	E-AST-01 E-AST-27
	CFG-02	Secure Baseline Configurations	10	Process	Annual	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21
	CFG-02.7	Approved Configuration Deviations	9	Process	Annual	E-AST-33
	CFG-03	Least Functionality	10	Technology	Annual	E-AST-12 E-AST-13 E-AST-14 E-AST-15 E-AST-16 E-AST-17 E-AST-18 E-AST-19 E-AST-20 E-AST-21
	CRY-01	Use of Cryptographic Controls	10	Data	Annual	E-CRY-01
	CRY-03	Transmission Confidentiality	10	Data	Annual	E-CRY-01
	CRY-05	Encrypting Data At Rest	10	Data	Annual	E-CRY-01

	CRY-08	Public Key Infrastructure (PKI)	9	Technology	Annual	
	CRY-09	Cryptographic Key Management	10	Technology	Annual	E-CRY-01 E-CRY-02
16	IAC-01	Identity & Access Management (IAM)	10	Technology	Annual	E-AST-01 E-IAM-05 E-IAM-12 E-MON-11
	IAC-01.2	Authenticate, Authorize and Audit (AAA)	9	Technology	Annual	E-IAM-06
	IAC-01.3	User & Service Account Inventories	10	Process	Annual	E-IAM-04 E-IAM-10 E-IAM-11
	IAC-06	Multi-Factor Authentication (MFA)	9	Technology	Quarterly	
	IAC-07	User Provisioning & De-Provisioning	10	Technology	Annual	E-HRS-12 E-HRS-18 E-HRS-19
	IAC-08	Role-Based Access Control (RBAC)	9	Technology	Annual	E-HRS-12 E-IAM-02
	IAC-10	Authenticator Management	10	Technology	Annual	
	IAC-10.11	Password Managers	8	Technology	Quarterly	
	IAC-10.8	Default Authenticators	10	Technology	Annual	
	IAC-15	Account Management	10	Technology	Quarterly	E-IAM-07 E-IAM-08
	IAC-15.7	System Account Reviews	10	Technology	Annual	E-IAM-07
	IAC-16	Privileged Account Management (PAM)	10	Technology	Quarterly	E-IAM-03
	IAC-16.1	Privileged Account Inventories	10	Technology	Annual	E-IAM-03
	IAC-17	Periodic Review of Account Privileges	10	Process	Annual	E-HRS-12 E-HRS-14 E-IAM-01
	IAC-20	Access Enforcement	10	Technology	Annual	
	IAC-21	Least Privilege	10	Technology	Annual	E-IAM-02 E-IAM-05 E-IAM-06
17	AST-01	Asset Governance	10	Process	Annual	E-AST-01
	AST-01.1	Asset-Service Dependencies	5	Process	Annual	E-BCM-09
	AST-01.2	Stakeholder Identification & Involvement	5	Process	Annual	E-CPL-03
	AST-02	Asset Inventories	10	Process	Annual	E-AST-04 E-AST-05 E-AST-07 E-AST-28
	AST-02.8	Data Action Mapping	9	Process	Semi-Annual	E-DCH-05
	AST-04	Network Diagrams & Data Flow Diagrams (DFDs)	10	Process	Annual	E-DCH-03 E-DCH-04 E-DCH-05
	AST-09	Secure Disposal, Destruction or Re-Use of Equipment	10	Process	Annual	E-AST-03
	AST-16	Bring Your Own Device (BYOD) Usage	10	Process	Annual	
	END-01	Endpoint Device Management (EDM)	10	Technology	Annual	E-AST-01 E-END-01
	END-02	Endpoint Protection Measures	9	Technology	Annual	
	END-04	Malicious Code Protection (Anti-Malware)	10	Technology	Annual	E-END-01 E-MON-02
	END-04.7	Always On Protection	9	Technology	Quarterly	
	END-08	Phishing & Spam Protection	10	Technology	Annual	
	MDM-01	Centralized Management Of Mobile Devices	10	Technology	Annual	
	MDM-03	Full Device & Container-Based Encryption	9	Technology	Annual	
	MDM-05	Remote Purging	9	Technology	Annual	
	MDM-06	Personally-Owned Mobile Devices	8	Technology	Annual	
	MDM-07	Organization-Owned Mobile Devices	8	Technology	Annual	
	MDM-11	Restricting Access To Authorized Technology Assets, Applications and/or Services (TAAS)	8	Technology	Annual	E-NET-06
18	EMB-01	Embedded Technology Security Program	10	Technology	Annual	E-AST-07

	EMB-06	Prevent Alterations	6	Technology	Annual	
	EMB-07	Embedded Technology Maintenance	6	Technology	Annual	
	EMB-10	Embedded Technology Reviews	8	Process	Annual	
19	MNT-01	Maintenance Operations	9	Process	Annual	E-MNT-02 E-MNT-04
	MNT-02	Controlled Maintenance	10	Process	Annual	E-MNT-04
	MNT-05	Remote Maintenance	9	Process	Annual	
20	VPM-01	Vulnerability & Patch Management Program (VPMP)	9	Process	Annual	E-MNT-03 E-THR-05 E-VPM-01
	VPM-02	Vulnerability Remediation Process	10	Process	Annual	E-RSK-03 E-RSK-04 E-VPM-01 E-VPM-09
	VPM-03	Vulnerability Ranking	8	Process	Annual	E-RSK-03 E-RSK-04 E-VPM-01 E-VPM-10
	VPM-05	Software & Firmware Patching	10	Technology	Quarterly	E-MNT-03 E-VPM-10
	VPM-06	Vulnerability Scanning	9	Process	Semi-Annual	E-VPM-05 E-VPM-11
21	AAT-01	Artificial Intelligence (AI) & Autonomous Technologies Governance	10	Process	Annual	E-AAT-01
	AAT-01.2	Trustworthy AI & Autonomous Technologies	10	Process	Annual	E-AAT-03
	AAT-02	Situational Awareness of AI & Autonomous Technologies	9	Process	Annual	
	AAT-02.3	Adequate Protections For AI & Autonomous Technologies	10	Process	Semi-Annual	
	AAT-10	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	10	Process	Annual	E-AAT-07 E-IAO-02
22	BCD-01	Business Continuity Management System (BCMS)	10	Process	Annual	E-BCM-01
	BCD-01.4	Recovery Time / Point Objectives (RTO / RPO)	5	Process	Annual	E-BCM-02 E-BCM-03
	BCD-01.5	Recovery Operations Criteria	6	Process	Annual	E-BCM-14
	BCD-02	Identify Critical Assets	9	Process	Annual	E-BCM-08
	BCD-02.1	Resume All Missions & Business Functions	8	Process	Annual	E-BCM-01
	BCD-02.2	Continue Essential Mission & Business Functions	8	Process	Annual	
	BCD-02.3	Resume Essential Missions & Business Functions	8	Process	Annual	
	BCD-11	Data Backups	10	Technology	Quarterly	E-BCM-10 E-BCM-11 E-BCM-12 E-BCM-13
	BCD-12	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	9	Technology	Annual	E-BCM-15
23	PRI-01	Data Privacy Program	10	Process	Annual	E-GOV-02 E-GOV-08
	PRI-01.11	Reasonable Data Privacy Practices	9	Process	Annual	
	PRI-02	Data Privacy Notice	7	Process	Annual	E-PRI-08
	PRI-03	Choice & Consent	7	Process	Semi-Annual	
	PRI-04	Restrict Collection To Identified Purpose	7	Data	Annual	E-PRI-02
	PRI-05.5	Inventory of Personal Data (PD)	8	Data	Annual	E-AST-08
	PRI-06	Data Subject Empowerment	6	Data	Annual	E-PRI-06
	PRI-14	Documenting Data Processing Activities	8	Process	Semi-Annual	
	PRI-17	Data Subject Communications	6	Process	Annual	
	RSK-10	Data Protection Impact Assessment (DPIA)	9	Process	Annual	E-PRI-04
24	PES-01	Physical & Environmental Protections	9	Process	Annual	E-PES-01 E-PES-05
	PES-01.1	Physical Security Plan (PSP)	4	Process	Annual	E-PES-04

	PES-01.2	Zone-Based Physical Security	3	Process	Annual	E-PES-11
	PES-02	Physical Access Authorizations	7	Process	Annual	E-HRS-28 E-PES-03 E-PES-05 E-PES-10
	PES-02.1	Role-Based Physical Access	9	Facility	Annual	E-PES-03 E-PES-05 E-PES-10
	PES-03	Physical Access Control	10	Facility	Annual	E-PES-05 E-PES-06 E-PES-07 E-PES-08 E-PES-09
	PES-04	Physical Security of Offices, Rooms & Facilities	10	Facility	Annual	
	PES-05	Monitoring Physical Access	7	Process	Semi-Annual	E-PES-05
	PES-06	Visitor Control	9	Facility	Annual	E-PES-02
	PES-12	Equipment Siting & Protection	9	Facility	Annual	
25	SAT-01	Cybersecurity & Data Protection-Minded Workforce	8	Process	Annual	E-SAT-02 E-SAT-04 E-SAT-05
	SAT-02	Cybersecurity & Data Protection Awareness Training	8	People	Annual	E-SAT-02
	SAT-03	Role-Based Cybersecurity & Data Protection Training	8	People	Annual	E-SAT-05
26	THR-01	Threat Intelligence Program	8	Process	Annual	E-THR-04
	THR-03	Threat Intelligence Feeds	8	Process	Annual	E-THR-03
	THR-09	Threat Catalog	5	Process	Annual	E-THR-06
	THR-10	Threat Analysis	7	Process	Annual	E-THR-07
27	CPL-01.1	Non-Compliance Oversight	9	Process	Semi-Annual	E-CPL-05
	CPL-01.3	Ability To Demonstrate Conformity	8	Process	Annual	
	CPL-01.4	Conformity Assessment	9	Process	Annual	
	CPL-02.2	Periodic Audits	8	Process	Annual	
	CPL-03.2	Functional Review Of Cybersecurity & Data Protection Controls	8	Process	Quarterly	E-CPL-08
	GOV-15.5	Monitor Controls	8	Process	Annual	
	GOV-18	Quality Management System (QMS)	4	Process	Annual	
	GOV-19	Assurance	7	Process	Annual	
28	CPL-01.1	Non-Compliance Oversight	9	Process	Semi-Annual	E-CPL-05
	IAO-05	Plan of Action & Milestones (POA&M)	9	Process	Annual	E-RSK-03
	RSK-04.1	Risk Register	10	Process	Semi-Annual	E-RSK-03
	TPM-05.5	Third-Party Scope Review	10	Process	Annual	E-TPM-03
	TPM-08	Review of Third-Party Services	9	Process	Semi-Annual	E-TPM-03
	TPM-10	Managing Changes To Third-Party Services	8	Process	Annual	E-TPM-01
29	BCD-04	Contingency Plan Testing & Exercises	6	Process	Annual	E-BCM-06 E-BCM-07
	IRO-06	Incident Response Testing	9	Process	Annual	E-IRO-04
30	GOV-01.2	Status Reporting To Governing Body	5	Process	Annual	E-CPL-05 E-CPL-09 E-GOV-03 E-GOV-04 E-GOV-05 E-GOV-06 E-GOV-07 E-GOV-13
	GOV-01.3	Commitment To Continual Improvements	7	Process	Annual	
	GOV-05	Measures of Performance	6	Process	Annual	E-GOV-13
	GOV-05.1	Key Performance Indicators (KPIs)	6	Process	Annual	
	GOV-05.2	Key Risk Indicators (KRIs)	6	Process	Annual	E-GOV-13

Appendix B – SCRMS Defensible Evidence

From a defensible governance perspective, there is a necessity to have evidence artifacts. The following artifacts are from the SCF's **Evidence Request List (ERL)** and are associated with controls in the SCRMS:

#	ERL #	Area of Focus	Documentation Artifact	Artifact Description	SCF Control Mappings
1	E-GOV-01	Cybersecurity & Data Protection Management	Charter - Cybersecurity Program	Documented evidence of a charter to establish and resource the organization's cybersecurity program.	GOV-01
2	E-GOV-02	Cybersecurity & Data Protection Management	Charter - Data Privacy Program	Documented evidence of a charter to establish and resource the organization's data privacy program.	GOV-01 PRI-01
3	E-GOV-03	Cybersecurity & Data Protection Management	Charter - Cybersecurity Steering Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of cybersecurity management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.1 GOV-01.2
4	E-GOV-04	Cybersecurity & Data Protection Management	Charter - Data Privacy Steering Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of privacy management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.2 CPL-02
5	E-GOV-05	Cybersecurity & Data Protection Management	Charter - Audit Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of internal and external audit management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.2 CPL-02
6	E-GOV-06	Cybersecurity & Data Protection Management	Charter - Risk Committee	Documented evidence of an executive steering committee, or advisory board, that is formed to perform oversight of risk management decisions and is comprised of key cybersecurity, technology, risk, privacy and business executives.	GOV-01.2 CPL-02
7	E-GOV-07	Cybersecurity & Data Protection Management	Charter - Data Management Board (DMB)	Documented evidence of the organization's Data Management Board (DMB) charter and mission.	GOV-01.2

8	E-GOV-08	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Policies	Documented evidence of an appropriately-scoped cybersecurity & data protection policies. Policies are high-level statements of management intent from an organization's executive leadership that are designed to influence decisions and guide the organization to achieve the desired outcomes. Policies are enforced by standards and further implemented by procedures to establish actionable and accountable requirements.	GOV-02 PRI-01
9	E-GOV-09	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Standards	Documented evidence of an appropriately-scoped cybersecurity & data protection standards. Standards are mandatory requirements regarding processes, actions and configurations. Standards are intended to be granular and prescriptive to ensure Technology Assets, Applications and/or Services (TAAS) are designed and operated to include appropriate cybersecurity & data protection protections	GOV-02
10	E-GOV-10	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Controls	Documented evidence of an appropriately-scoped cybersecurity & data protection controls. Controls are technical, administrative or physical safeguards. Controls are the nexus used to manage risks through preventing, detecting or lessening the ability of a particular threat from negatively impacting business processes. Controls directly map to standards, since control testing is designed to measure specific aspects of how standards are actually implemented.	GOV-09 CPL-01 CPL-01.2 BCD-13 BCD-13.1 SEA-01.1 SEA-01.2
11	E-GOV-11	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Procedures	Documented evidence of an appropriate appropriately-scoped cybersecurity & data protection procedures. Procedures are a documented set of steps necessary to perform a specific task or process in conformance with an applicable standard. Procedures help address the question of how the organization actually operationalizes a policy, standard or control. The result of a procedure is intended to satisfy a specific control. Procedures are also commonly referred to as “control activities.”	GOV-02 OPS-01.1 BCD-13 BCD-13.1
12	E-GOV-12	Cybersecurity & Data Protection Management	Cybersecurity & Data Protection Policies & Standards Reviews	Documented evidence of a periodic review process for the organization's cybersecurity & data protection policies and standards to identify necessary updates.	GOV-03 SEA-01.1 SEA-01.2

13	E-GOV-13	Cybersecurity & Data Protection Management	Measures of Performance (Metrics)	Documented evidence of formal measure of performance that are used to track the health of the cybersecurity & data protection program (e.g., metrics, KPIs, KRIs).	GOV-01.2 GOV-05 GOV-05.2 CPL-02
14	E-GOV-14	Cybersecurity & Data Protection Management	Materiality Threshold Definition	Documented evidence of criteria to define the organization's materiality threshold.	GOV-16
15	E-GOV-15	Cybersecurity & Data Protection Management	Material Risks	Documented evidence of specific risks that are categorized as material risks.	GOV-16.1 RSK-13 RSK-13.2
16	E-GOV-16	Cybersecurity & Data Protection Management	Material Threats	Documented evidence of specific threats that are categorized as material threats.	GOV-16.2
17	E-GOV-18	Cybersecurity & Data Protection Management	Exception Management	Documented evidence of authorized exceptions to standards (e.g., configurations, practices, etc.)	CRY-01.1 GOV-02.1
18	E-GOV-19	Cybersecurity & Data Protection Management	Operationalizing Cybersecurity & Data Protection Practices	Documented evidence of personnel management actions to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their control.	GOV-15
19	E-GOV-20	Cybersecurity & Data Protection Management	Compensating Controls	Documented evidence of compensating controls (e.g., countermeasure to reduce risk associated with control deficiencies).	CFG-02.9 RSK-06.2
20	E-AAT-01	Artificial Intelligence (AI) & Autonomous Technologies Governance	Artificial Intelligence and Autonomous Technologies (AAT) Governance Program	Documented evidence of a governance program for Artificial Intelligence and Autonomous Technologies (AAT).	AAT-01
21	E-AAT-03	Artificial Intelligence (AI) & Autonomous Technologies Governance	Secure Development Practices for Artificial Intelligence and Autonomous Technologies (AAT).	Documented evidence of industry-recognized secure practices to develop and maintain trustworthy Artificial Intelligence and Autonomous Technologies (AAT).	AAT-01.2

22	E-AAT-07	Artificial Intelligence (AI) & Autonomous Technologies Governance	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) Practices	Documented evidence of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices.	AAT-10
23	E-AST-01	Asset Management	IT Asset Management (ITAM)	Documented evidence of an IT Asset Management (ITAM) program that addresses the due diligence and due care activities associated with maintaining both secure, compliance and resilient Technology Assets, Applications and/or Services (TAAS).	AST-01 AST-03 AST-03.1 AST-10 CFG-05 END-01 IAC-01 IAC-02.2 MON-03 MON-16.4
24	E-AST-02	Asset Management	Asset Scoping Guidance	Documented evidence of an asset scoping guidance. This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on defining in-scope Technology Assets, Applications, Services and/or Data (TAASD) (including third-parties).	AST-04.1 AST-04.2 AST-04.3 CPL-01.2 IAO-01.1
25	E-AST-03	Asset Management	Asset Disposal Evidence	Documented evidence of asset disposal/destruction (e.g., asset tracking by serial # for shredding, degaussing, etc.).	AST-09 DCH-08 DCH-09 DCH-09.1
26	E-AST-04	Asset Management	Asset Inventories - Hardware	Documented evidence of an inventory of the organization's technology hardware assets.	AST-02
27	E-AST-05	Asset Management	Asset Inventories - Software	Documented evidence of an inventory of the organization's software assets.	AST-02
28	E-AST-06	Asset Management	Asset Inventories - Cloud Service Provider (CSP)	Documented evidence of an inventory of the organization's cloud-based services (e.g., SaaS, IaaS, PaaS, etc.).	CLD-01 CLD-09 TPM-01.1
29	E-AST-07	Asset Management	Cyber-Physical Systems (CPS)	Documented evidence of an inventory of the organization's physical assets that process functions based on software and networks.	AST-02 EMB-01
30	E-AST-08	Asset Management	Asset Inventories - Sensitive / Regulated Data	Documented evidence of an inventory of the organization's sensitive/regulated data (including systems where sensitive/regulated data is stored, processed and/or transmitted) that	CLD-10 DCH-01.3 DCH-06.2 BCD-11.2 PRI-05.5

				contains sufficient information to determine the potential impact in the event of a data loss incident.	
31	E-AST-11	Asset Management	Data Retention Program	Documented evidence of a formal data retention program that governs the retention and destruction of data types.	DCH-18 MON-10 PRI-05
32	E-AST-12	Asset Management	Secure Baseline Configurations Reviews	Documented evidence of a review process to ensure Secure Baseline Configurations (SBC) are current and applicable (e.g., system configuration settings and associated documentation).	CFG-02 CFG-02.1 CFG-02.5 CFG-03 NET-04 NET-04.1 NET-04.6
33	E-AST-13	Asset Management	Secure Baseline Configurations - Cloud-Based Services	Documented evidence of secure baseline configurations for all deployed types of cloud-based services or applications.	CFG-02 CFG-03 CFG-02.5
34	E-AST-14	Asset Management	Secure Baseline Configurations - Databases	Documented evidence of secure baseline configurations for all deployed types of databases.	CFG-02 CFG-03 CFG-02.5
35	E-AST-15	Asset Management	Secure Baseline Configurations - Embedded Technologies	Documented evidence of secure baseline configurations for all deployed types of embedded technologies.	CFG-02 CFG-03 CFG-02.5
36	E-AST-16	Asset Management	Secure Baseline Configurations - Major Applications	Documented evidence of secure baseline configurations for all deployed types of major applications.	CFG-02 CFG-03 CFG-02.5
37	E-AST-17	Asset Management	Secure Baseline Configurations - Minor Applications	Documented evidence of secure baseline configurations for all deployed types of minor applications.	CFG-02 CFG-03 CFG-02.5
38	E-AST-18	Asset Management	Secure Baseline Configurations - Mobile Devices	Documented evidence of secure baseline configurations for all deployed types of mobile devices.	CFG-02 CFG-03 CFG-02.5

39	E-AST-19	Asset Management	Secure Baseline Configurations - Network Devices	Documented evidence of secure baseline configurations for all deployed types of network devices.	CFG-02 CFG-02.5 CFG-03 NET-04 NET-04.1
40	E-AST-20	Asset Management	Secure Baseline Configurations - Server Class Systems	Documented evidence of secure baseline configurations for all deployed types of server-class operating systems.	CFG-02 CFG-02.5 CFG-03 CFG-03.2
41	E-AST-21	Asset Management	Secure Baseline Configurations - Workstation Class Systems	Documented evidence of secure baseline configurations for all deployed types of workstation-class operating systems.	CFG-02 CFG-02.5 CFG-03 CFG-03.2 CFG-05
42	E-AST-23	Asset Management	Geolocation Inventory	Documented evidence of designated internal and third-party facilities where organizational data is stored, transmitted and/or processed.	BCD-02.4 CLD-09 DCH-19 DCH-24
43	E-AST-27	Asset Management	Configuration Management	Documented evidence of standardized configuration management practices.	CFG-01
44	E-AST-28	Asset Management	Software Licenses	Documented evidence of software license inventories.	AST-02
45	E-AST-33	Asset Management	Tailored Baselines	Documented evidence exists for tailored baseline configurations to address unique business and/or technical requirements (e.g., kiosk, hazardous environments, etc.).	AST-02.4 CFG-02.5 CFG-02.7 CFG-02.9
46	E-BCM-01	Business Continuity	Continuity of Operations Plan (COOP)	Documented evidence of a Continuity of Operations Plan (COOP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards. This involves internal and external stakeholders for incident response, disaster recovery and business continuity support requirements.	BCD-01 BCD-01.1 BCD-01.2 BCD-01.6 BCD-02.1 SEA-01.2
47	E-BCM-02	Business Continuity	Recovery Time Objectives (RTOs)	Documented evidence of Recovery Time Objectives (RTOs) that guide Continuity of Operations Plan (COOP)-related operations.	BCD-01.4

48	E-BCM-03	Business Continuity	Recovery Point Objectives (RPOs)	Documented evidence of Recovery Point Objectives (RPOs) that guide Continuity of Operations Plan (COOP)-related operations.	BCD-01.4
49	E-BCM-06	Business Continuity	COOP Testing	Documented evidence of a Continuity of Operations Plan (COOP)-related testing activity.	BCD-03.1 BCD-04
50	E-BCM-07	Business Continuity	COOP Training	Documented evidence of a Continuity of Operations Plan (COOP)-related training activity.	BCD-03 BCD-04
51	E-BCM-08	Business Continuity	COOP Criticality Analysis	Documented evidence of a Continuity of Operations Plan (COOP)-related criticality analysis.	BCD-02 TDA-06.1
52	E-BCM-09	Business Continuity	COOP Dependency Analysis	Documented evidence of a Continuity of Operations Plan (COOP)-related dependency analysis for Technology Assets, Applications, Services and/or Data (TAASD) (including facilities and third-parties).	AST-01.1 RSK-02 RSK-02.1
53	E-BCM-10	Business Continuity	Backups	Documented evidence of a Continuity of Operations Plan (COOP)-related data backup scheme that demonstrates the methods of data backup (including protection measures) for all data types to ensure business continuity requirements.	BCD-11 BCD-11.1
54	E-BCM-11	Business Continuity	Backups - Local	Documented evidence of event logs for the on-site / local data backup solution.	BCD-11 BCD-11.2
55	E-BCM-12	Business Continuity	Backups - Remote	Documented evidence of event logs for the off-site / remote data backup solution.	BCD-11 BCD-11.2 BCD-11.6
56	E-BCM-13	Business Continuity	Backups - Recovery Activities	Documented evidence of recovery activities (successful and failed).	BCD-11 BCD-11.1

57	E-BCM-14	Business Continuity	Recovery Operations Criteria	Documented evidence of specific criteria to activate Business Continuity / Disaster Recovery (BC/DR) plans.	BCD-01.5
58	E-BCM-15	Business Continuity	Restoration Events	Documented evidence of system, application and/or data recovery events. This can include random testing of data backups to ensure recovery methods are viable.	BCD-11.5 BCD-12
59	E-CAP-01	Capacity Management	Capacity Planning	Documented evidence of proactive capacity planning to meet expected and anticipated future technology-related capacity and/or performance requirements.	CAP-01 CAP-03
60	E-CAP-04	Capacity Management	Dynamic Expansion Capabilities	Documented evidence of dynamic expansion capabilities (e.g., elastic expansion) to meet capacity and/or performance requirements for critical Technology Assets, Applications and/or Services (TAAS).	CAP-05
61	E-CHG-01	Change Management	Business Impact Analysis (BIA)	Documented evidence of a Business Impact Analysis (BIA) for proposed changes.	RSK-08 TDA-06.1
62	E-CHG-02	Change Management	Charter - Change Control Board (CCB)	Documented evidence of the organization's Change Control Board (CCB) charter and mission to govern the organization's change control processes.	CHG-01 CHG-02 CHG-02.1
63	E-CHG-04	Change Management	Evidence of Cybersecurity / Data Privacy Reviews	Documented evidence of Change Control Board (CCB) meeting-related cybersecurity and/or data privacy reviews for proposed change(s).	CHG-02.3 CHG-03
64	E-CHG-05	Change Management	Change Control Records	Documented evidence of change control records (including test results, when applicable).	CHG-02 CHG-02.2
65	E-CPL-01	Compliance	Statutory, Regulatory & Contractual Obligations	Documented evidence of applicable statutory, regulatory and/or contractual obligations for cybersecurity & data privacy controls.	CPL-01 MON-03
66	E-CPL-02	Compliance	Defined Compliance Scope (DCS)	Documented evidence of a formal scoping document that identifies applicable statutory, regulatory and/or contractual obligations for the organization. Defines the affected Lines of Business (LOB),	AST-04.1 AST-04.2 AST-04.3 CPL-01.2

				internal / external stakeholders and facilities for the specific scope of compliance obligations.	
67	E-CPL-03	Compliance	Shared Responsibility Matrix (SRM) / Controls Responsibility Matrix (CRM)	Documented evidence of a Controls Responsibility Matrix (CRM), or similar documentation, that identifies the stakeholder involved in executing assigned controls (e.g., Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix).	AST-01.2 AST-03 CLD-06.1 TPM-05.4
68	E-CPL-05	Compliance	Internal Audit (IA) Findings	Documented evidence of a centrally-managed and prioritized repository Internal Audit (IA) findings.	CPL-01.1 CPL-03 GOV-01.2
69	E-CPL-06	Compliance	Manufacturer Disclosure Statement for Medical Device Security (MDS2)	Documented Manufacturer Disclosure Statement for Medical Device Security (MDS2) that communicates information about medical device cybersecurity & data privacy characteristics to current device owners and potential buyers. *[note MDS2 is specific to medical device manufacturers]*	TDA-01.1 TDA-02.1 TDA-02.5 TDA-04 TDA-04.1 TPM-04 TPM-04.2
70	E-CPL-08	Compliance	Functional Review of Cybersecurity Controls	Documented evidence of control testing to ensure cybersecurity controls function as expected.	CPL-03.2
71	E-CPL-09	Compliance	Non-Compliance Oversight Reporting	Documented evidence of governance oversight reporting of non-compliance to the organization's executive leadership.	CPL-02 GOV-01.2
72	E-CRY-01	Cryptographic Protections	Cryptographic Protections	Documented evidence of organization-approved cryptographic solutions and modules for both data at rest and in transit.	CRY-01 CRY-03 CRY-04 CRY-05 CRY-09 CRY-09.1 CRY-09.2 DCH-01 DCH-01.2
73	E-CRY-02	Cryptographic Protections	Cryptographic Key Management	Documented evidence of cryptographic key management practices.	CRY-09

74	E-DCH-01	Data Protection	Data Classification Scheme	Documented evidence of an organization-specific data classification scheme.	AST-04.1 DCH-02
75	E-DCH-02	Data Protection	Data Handling Practices	Documented evidence of an organization-specific data handling practices (e.g., guidance specific the data classification scheme).	AST-04.1 DCH-01.1 DCH-01.2 DCH-01.4 DCH-02 DCH-06
76	E-DCH-03	Data Protection	Network Diagram - Global System View (GSV)	Documented evidence of a high-level network diagram that provides a conceptual, logical depiction of the network(s) to describe the interconnections of the systems/applications/services, including internal and external interfaces.	AST-04 NET-02
77	E-DCH-04	Data Protection	Network Diagram - Low Level	Documented evidence of a low-level network diagram that provides a detailed, logical depiction of assets on the network(s).	AST-04 NET-02
78	E-DCH-05	Data Protection	Data Flow Diagram (DFD)	Documented evidence of a Data Flow Diagram (DFD) that accurately identifies where sensitive/regulated data is stored, transmitted and/or processed.	AST-02.8 AST-04 NET-02
79	E-DCH-06	Data Protection	Third-Party Inventories	Documented evidence of an inventory of External Service Providers (ESP), contractors, vendors, etc. that directly or indirectly impact the organization's Technology Assets, Applications, Services and/or Data (TAASD).	TPM-01.1
80	E-DCH-08	Data Protection	Authorization Documentation	Documented evidence of that identifies authorized users and processes acting on behalf of authorized users.	CFG-08 DCH-01.4
81	E-DCH-09	Data Protection	Assigned Responsibilities	Documented evidence of data stewardship being assigned and communicated to individuals entrusted with sensitive and/or regulated data.	CRY-01 DCH-01.1 DCH-14
82	E-DCH-15	Data Protection	Geolocation Restrictions	Documented evidence of geolocation restrictions placed on specific types of sensitive and/or regulated data for where that data can be stored and/or processed.	CLD-09

83	E-SAT-02	Education	Initial User Training	Documented evidence of initial user training for cybersecurity and/or data privacy topics.	SAT-01 SAT-02 SAT-02.2 SAT-04 HRS-05.7
84	E-SAT-04	Education	Recurring User Training	Documented evidence of recurring (e.g., annual) user training for cybersecurity and/or data privacy topics.	SAT-01 SAT-03.4 SAT-03.6 SAT-03.7 SAT-04 HRS-05.7 THR-05
85	E-SAT-05	Education	Role-Based Training	Documented evidence of specialized user training for privileged users, executives, individuals who handle sensitive/regulated data, etc.	DCH-14 SAT-01 SAT-03 SAT-03.4 SAT-03.5 SAT-04 THR-05
86	E-MON-01	Event Log Monitoring	Event Log Review & Analysis	Documented evidence of a capability to perform security event log review and analysis (e.g., system monitoring records, continuous monitoring strategy, etc.).	MON-01 MON-01.1 MON-01.2 MON-01.3 MON-01.4 MON-01.8 MON-02 MON-02.2
87	E-MON-02	Event Log Monitoring	Malware Activity	Documented evidence of malware activity being logged and included as part of the centralized event log collection and review/analysis process.	MON-01.8 MON-02.2 END-04.3
88	E-MON-05	Event Log Monitoring	Centralized Event Log Collection	Documented evidence of security-relevant activities being logged and included as part of the centralized event log collection and review/analysis process.	MON-01.2 MON-01.8 MON-02 MON-02.2 MON-02.1
89	E-MON-06	Event Log Monitoring	Automated Event Escalation & Reporting	Documented evidence of a capability for selected events to alert applicable personnel, or roles, based on the type of event. This can be demonstrated by the configuration of a Security Incident Event Manager (SIEM), or similar technology, that helps automate event log analysis and reporting.	MON-01 MON-01.1 MON-01.3 MON-01.4 MON-01.12
90	E-MON-07	Event Log Monitoring	Situational Awareness	Documented evidence of the organization leveraging knowledge of event log generation to gain situational awareness of cross-domain activities (e.g., technology issues, security events, policy violations, service provider activities, remote workforce activities, physical security events, etc.).	MON-01 MON-01.1 MON-01.3 MON-01.4 MON-02.1 MON-11.3 MON-16 MON-16.1

					MON-16.2 MON-16.3
91	E-MON-11	Event Log Monitoring	System Authenticator Types	Documented evidence of the list of authorized system authenticator types.	IAC-01
92	E-HRS-01	Human Resources	Position Categorization	Documented evidence of a discrete roles for cybersecurity & data privacy functions (e.g., position categorization).	GOV-04 HRS-01 HRS-02 HRS-03 HRS-03.1
93	E-HRS-02	Human Resources	Assigned Roles - Application Developers	List of employed or contract personnel assigned to application development roles.	HRS-02 HRS-02.1 HRS-03 OPS-01
94	E-HRS-03	Human Resources	Assigned Roles - Cybersecurity Staff	List of employed or contract personnel assigned to cybersecurity roles.	HRS-02 HRS-02.1 HRS-03 OPS-01
95	E-HRS-04	Human Resources	Assigned Roles - Data Privacy Staff	List of employed or contract personnel assigned to data privacy roles.	HRS-02 HRS-02.1 HRS-03 OPS-01
96	E-HRS-05	Human Resources	Role Assignment - CISO	Documented evidence of a formal role assignment to the Chief Information Security Officer (CISO) position.	GOV-04
97	E-HRS-06	Human Resources	Role Assignment - COO	Documented evidence of a formal role assignment to the Chief Operations Officer (COO) position.	GOV-04
98	E-HRS-07	Human Resources	Role Assignment - CIO	Documented evidence of a formal role assignment to the Chief Information Officer (CIO) position.	GOV-04
99	E-HRS-08	Human Resources	Role Assignment - CPO	Documented evidence of a formal role assignment to the Chief Privacy Officer (CPO) position.	GOV-04 PRI-01.1

100	E-HRS-09	Human Resources	Role Assignment - CRO	Documented evidence of a formal role assignment to the Chief Risk Officer (CRO) position.	GOV-04
101	E-HRS-10	Human Resources	Role Assignment - DPO	Documented evidence of a formal role assignment to Data Protection Officer (DPO) positions.	GOV-04 PRI-01.4
102	E-HRS-11	Human Resources	Role Assignment - Sensitive / Regulated Data	Documented evidence of a formal role assignment to personnel who are cleared to handle sensitive/regulated data.	HRS-02 HRS-02.1 HRS-03
103	E-HRS-12	Human Resources	Role Review	Documented evidence of a formal review process to ensure personnel roles currently reflect business needs.	IAC-07 IAC-07.1 IAC-08 IAC-17
104	E-HRS-13	Human Resources	Defined Cybersecurity & Data Privacy Responsibilities	Documented evidence of a role-based cybersecurity & data privacy responsibilities to ensure personnel are both educated on the role and are responsible for the associated control execution.	CHG-04 GOV-04 HRS-03 HRS-03.1 OPS-01
105	E-HRS-14	Human Resources	Responsibilities Review	Documented evidence of a formal review process to ensure assigned responsibilities currently reflect business needs for the assigned role.	IAC-17
106	E-HRS-15	Human Resources	Organization Chart	Current and accurate organization chart that depicts logical staff hierarchies.	GOV-04 GOV-04.1 GOV-04.2 HRS-01 OPS-01
107	E-HRS-16	Human Resources	Access Agreements	Documented evidence of personnel management practices protecting sensitive/regulated data through formal access agreements.	HRS-03.1 HRS-05 HRS-06 HRS-10
108	E-HRS-17	Human Resources	Background Checks	Documented evidence of personnel screening practices, which centers around some form of formalized background check process.	HRS-04 HRS-04.1
109	E-HRS-18	Human Resources	Provisioning Checklist (Onboarding)	Documented evidence of personnel management practices to formally onboard personnel into their assigned roles.	HRS-03 HRS-03.1 HRS-04.2 HRS-05.7 HRS-10

					IAC-07 IAC-28
110	E-HRS-19	Human Resources	Deprovisioning Checklist (Offboarding)	Documented evidence of personnel management practices to formally offboard personnel from their assigned roles due to employment termination or role change.	HRS-06.2 HRS-09 HRS-09.1 HRS-09.2 HRS-09.3 IAC-07 IAC-07.1 IAC-07.2
111	E-HRS-21	Human Resources	Position Competency Requirements	Documented evidence of personnel management practices to define minimum competency requirements for cybersecurity & data privacy-related roles.	HRS-03.2 HRS-04 HRS-04.1
112	E-HRS-22	Human Resources	Rules of Behavior	Documented evidence of personnel management practices to define "acceptable use" or "rules of behavior" criteria that specify acceptable and unacceptable user behaviors.	HRS-02 HRS-02.1 HRS-03 HRS-05 HRS-05.1 HRS-05.2 HRS-05.3 HRS-05.4 HRS-05.5 HRS-10
113	E-HRS-23	Human Resources	Critical Cybersecurity & Data Privacy Skills	Documented evidence of personnel management practices to formally identify critical cybersecurity skills needed to support business operations.	HRS-03.2 HRS-13
114	E-HRS-24	Human Resources	Critical Cybersecurity & Data Privacy Skill Gaps	Documented evidence of personnel management practices to formally identify critical cybersecurity & data privacy skill gaps.	HRS-13 HRS-13.1
115	E-HRS-27	Human Resources	Personnel Sanctions	Documented evidence of personnel management practices to formally sanction unacceptable behavior(s).	HRS-01 HRS-07 OPS-01
116	E-HRS-28	Human Resources	Authorized Personnel Access List	Documented evidence of an authorized personnel access list.	HRS-03 PES-02

117	E-HRS-29	Human Resources	Personnel Actions Documentation	Documented evidence of notifications or records of recently transferred, separated, or terminated employees.	HRS-07 HRS-08 HRS-09
118	E-IAM-01	Identity & Access Management	Access Permission Review	Documented evidence of periodic access permission reviews.	IAC-17
119	E-IAM-02	Identity & Access Management	Defined Roles & Authorizations (RBAC)	Documented evidence of defined access control-specific roles (e.g., Role Based Access Control (RBAC)) that affect both logical and physical access authorizations.	CFG-05 CHG-04 DCH-03 END-03 IAC-08 IAC-21
120	E-IAM-03	Identity & Access Management	Privileged User Inventory	Documented evidence of an inventory of privileged users across Technology Assets, Applications and/or Services (TAAS) (internal and external).	IAC-16 IAC-16.1
121	E-IAM-04	Identity & Access Management	User & Service Inventory	Documented evidence of an inventory of authorized users and services.	IAC-01.3
122	E-IAM-05	Identity & Access Management	Identity & Access Management (IAM) Function	Documented evidence of an Identity & Access Management (IAM), or similar function, that facilitates the implementation of identification and access management controls.	IAC-01 IAC-02 IAC-02.2 IAC-03 IAC-03.5 IAC-04 IAC-05 IAC-21 IAC-28
123	E-IAM-06	Identity & Access Management	Authenticate, Authorize and Audit (AAA) Solution	Documented evidence of an Authenticate, Authorize and Audit (AAA) solution (on-premises and hosted by External Service Providers (ESP)).	IAC-01.2 IAC-02 IAC-02.2 IAC-03 IAC-03.5 IAC-04 IAC-05 IAC-21 IAC-28
124	E-IAM-07	Identity & Access Management	Account Management Compliance Reviews	Documented evidence of account management compliance reviews.	IAC-15 IAC-15.7

125	E-IAM-08	Identity & Access Management	Conditions for Group / Role Membership	Documented evidence of conditions for group and role membership.	IAC-15 IAC-15.5
126	E-IAM-10	Identity & Access Management	Active Accounts	Documented evidence of active system accounts and the name of the individual associated with each account.	IAC-01.3
127	E-IAM-11	Identity & Access Management	Recently Disabled Accounts	Documented evidence of list of recently disabled system accounts along with the name of the individual associated with each account.	IAC-01.3
128	E-IAM-12	Identity & Access Management	Account Management Documentation	Documented evidence of list of account management practices.	IAC-01
129	E-IAM-14	Asset Management	Remote Access Authorizations	Documented evidence of authorization for users to connect via remote access methods.	NET-14 NET-14.5 NET-14.6
130	E-IRO-01	Incident Response	Incident Response Plan (IRP)	Documented evidence of a Incident Response Plan (IRP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	IRO-01 IRO-02.4 IRO-02.5 IRO-04 IRO-06.1 IRO-07 IRO-08 IRO-10 IRO-10.2
131	E-IRO-02	Incident Response	Indicators of Compromise (IOC)	Documented evidence of defined Indicators of Compromise (IOC).	MON-11.3 MON-16 MON-16.1 MON-16.2 MON-16.3 IRO-03
132	E-IRO-03	Incident Response	Incident Tracking	Documented evidence of a centralized repository to track cybersecurity & data privacy incidents.	IRO-02 IRO-09
133	E-IRO-04	Incident Response	IRP Testing	Documented evidence of an Incident Response Plan (IRP)-related testing activity.	IRO-06

134	E-IRO-08	Incident Response	Root Cause Analysis (RCA)	Documented evidence of a Root Cause Analysis (RCA) from any Incident Response Plan (IRP)-related training, testing or significant incident.	IRO-13
135	E-IRO-09	Incident Response	Formally Assigned Incident Response Roles & Responsibilities	Documented evidence of the establishment of a formally-assigned, integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	IRO-07 IRO-16
136	E-IRO-11	Incident Response	Incident Reporting Capability	Documented evidence of a capability to provide situational awareness of incidents to internal stakeholders and generated necessary reporting to affected clients, applicable third-parties and regulatory authorities.	IRO-10 IRO-10.2
137	E-IRO-13	Incident Response	Incident Response Records	Documented evidence of records of response to cybersecurity and/or data protection incidents.	IRO-09
138	E-IAO-01	Information Assurance	Information Assurance Program (IAP)	Documented evidence of a Information Assurance Program (IAP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	IAO-01 IAO-02.4
139	E-IAO-02	Information Assurance	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	Documented evidence of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable AI-related testing, identification of incidents and information sharing.	AAT-10
140	E-IAO-03	Information Assurance	Pre-Production Controls Testing	Documented evidence of pre-production cybersecurity & data protection controls testing 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.	IAO-02 IAO-02.4 IAO-03.2
141	E-IAO-04	Information Assurance	Security Assessment Plan	Documented evidence of a plan to conduct security assessments.	IAO-02
142	E-IAO-05	Information Assurance	Security Assessment Report	Documented evidence of a report on security assessments.	IAO-02.4

143	E-MNT-02	Maintenance	Maintenance Plan	Documented evidence of a Maintenance Plan. This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	MNT-01
144	E-MNT-03	Maintenance	Patch Management	Documented evidence of maintenance activities for Technology Assets, Applications and/or Services (TAAS) (e.g., patch management).	VPM-01 VPM-04 VPM-05
145	E-MNT-04	Maintenance	Maintenance Activities	Documented evidence of maintenance activities for the organization's Technology Assets, Applications and/or Services (TAAS).	MNT-01 MNT-02 MNT-03 MNT-03.1
146	E-NET-01	Network Security	Content / DNS Filtering	Documented evidence of the methods that content / DNS filtering is implemented to prevent Internet traffic from prohibited content and/or hostile web sites.	NET-18 NET-18.1
147	E-NET-03	Network Security	Work From Anywhere (WFA) Guidance (remote workers)	Documented evidence of administrative and technical measures that are enforced at "alternate work sites" which includes working from home or working while traveling on business.	NET-14 NET-14.5
148	E-NET-04	Network Security	Network Security Controls (NSC)	Documented evidence of the organization's network security controls (e.g., boundary protections, content filtering, wireless infrastructure, etc.).	NET-01
149	E-NET-06	Network Security	Authorized Network Connections	Documented evidence of third-party Technology Assets, Applications and/or Services (TAAS) authorized to connect to organizational TAAS, including remote access authorizations.	NET-04 NET-05 NET-05.1 MDM-11
150	E-NET-07	Network Security	External System Accessibility	Documented evidence of a list of Technology Assets, Applications and/or Services (TAAS) accessible from third-party entities.	NET-04 NET-04.1
151	E-NET-08	Network Security	Internal Boundaries	Documented evidence of key internal boundaries.	NET-03
152	E-NET-09	Network Security	Network Access Control Points	Documented evidence of network access control points.	NET-03 NET-05.1 NET-14.3

153	E-NET-10	Network Security	Information Flow Control	Documented evidence of information flow control mechanisms (e.g., Access Control Lists, etc.).	NET-04 NET-04.1
154	E-PES-01	Physical Security	Environmental Monitoring	Documented evidence of environmental monitoring (e.g., water leaks, temperature, humidity, etc.)	PES-01 PES-07 PES-07.5 PES-08 PES-09
155	E-PES-02	Physical Security	Visitor Logbook	Documented evidence of a visitor management and logging visitor activities.	PES-03.3 PES-06 PES-06.4
156	E-PES-03	Physical Security	Defined Physical Security Roles	Documented evidence of defined physical access control-specific roles that limit physical access to rooms and/or facilities.	PES-02 PES-02.1
157	E-PES-04	Physical Security	Physical Security Plan	Documented evidence of a physical security plan.	PES-01.1
158	E-PES-05	Physical Security	Physical Security Operations	Documented evidence of the organization's physical security capabilities as it pertains to operating and monitoring Physical Access Control (PAC) mechanisms.	PES-01 PES-02 PES-02.1 PES-03 PES-05
159	E-PES-06	Physical Security	Physical Access Control Logs	Documented evidence of physical access control logs or records.	PES-03
160	E-PES-07	Physical Security	Physical Access Control Devices	Documented evidence of Physical Access Control (PAC) mechanisms.	PES-03
161	E-PES-08	Physical Security	Physical Access Control Device Inventories	Documented evidence of inventory records of physical access control devices.	PES-03
162	E-PES-09	Physical Security	Key & Combination Changes	Documented evidence of key and lock combination changes.	PES-03

163	E-PES-10	Physical Security	Physical Access Authorizations	Documented evidence of physical access authorization activities (e.g., list reviews, termination changes, etc.).	PES-02 PES-02.1
164	E-PES-11	Physical Security	Physical Security Zones	Documented evidence of security safeguards controlling access to designated physical security zones within facilities.	PES-01.2
165	E-PRI-02	Privacy	Authorized Use	Documented evidence of authorized use definitions for privacy-related data operations.	PRI-04 PRI-04.1 PRI-05 PRI-05.1
166	E-PRI-04	Privacy	Data Protection Impact Assessment (DPIA)	Documented evidence of Data Protection Impact Assessment (DPIA).	RSK-10
167	E-PRI-06	Privacy	Data Subject Access	Documented evidence of how data subject access requests are handled that includes intake through remediation.	PRI-06
168	E-PRI-08	Privacy	Data Privacy Notice	Documented evidence of a publicly-accessible data privacy notice.	PRI-02
169	E-PRM-01	Resource Management	Cybersecurity Business Plan (CBP)	Documented evidence of a cybersecurity-specific business plan that documents a strategic plan and discrete objectives.	GOV-08 PRM-01.1 PRM-03
170	E-PRM-02	Resource Management	Portfolio Roadmap	Documented evidence of the organization's roadmap for implementing cybersecurity-related initiatives and technologies.	PRM-01 PRM-02 PRM-03
171	E-PRM-03	Resource Management	Secure Development Lifecycle (SDLC)	Documented evidence of a secure development lifecycle that the organization utilizes for new initiatives or significant changes to existing initiatives to ensure cybersecurity & data privacy principles are identified and implemented by default.	PRM-04 PRM-05 PRM-06 PRM-07

172	E-PRM-04	Resource Management	Targeted Maturity Level	Documented evidence of a targeted level of control maturity from a Capability Maturity Model (CMM).	PRM-01.2
173	E-PRM-05	Resource Management	System Design Document (SDD)	Documented evidence of a System Design Document (SDD) focuses on how a Technology Asset, Application and/or Service (TAAS) is built (e.g., architecture, components, data flow, functions, etc.).	PRM-04 PRM-05 PRM-06 PRM-07
174	E-PRM-06	Resource Management	Quarterly Business Review (QBR)	Documented evidence of a Quarterly Business Review (QBR), or similar process, to provide recurring status reports on the current state of the cybersecurity and data protection program.	GOV-01.1
175	E-RSK-01	Risk Management	Risk Management Program (RMP)	Documented evidence of a Risk Management Program (RMP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	RSK-01 RSK-01.1 RSK-02 RSK-12
176	E-RSK-02	Risk Management	Supply Chain Risk Management (SCRM) Plan	Documented evidence of a Supply Chain Risk Management (SCRM) Plan. This is program-level documentation in the form of a playbook, concept of operations or a similar format provides guidance on organizational practices that support existing policies and standards.	IRO-10.4 RSK-09 TPM-03 TPM-05 TPM-05.2
177	E-RSK-03	Risk Management	Plan of Actions & Milestones (POA&M) / Risk Register	Documented evidence of a POA&M, or risk register, that tracks control deficiencies from identification through remediation.	AST-02.4 CPL-02 IAO-05 RSK-04.1 RSK-06 RSK-06.1 RSK-06.2 VPM-02 VPM-03
178	E-RSK-04	Risk Management	Cybersecurity Risk Assessment (RA)	Documented evidence of a cybersecurity-specific risk assessment.	RSK-02 RSK-02.1 RSK-03 RSK-04 RSK-05 VPM-02 VPM-03
179	E-RSK-05	Risk Management	Supply Chain Risk Assessment (SCRA)	Documented evidence of supply chain-specific risk assessment that evaluates risks that are specific to its supply chain.	RSK-09.1

180	E-RSK-06	Risk Management	Risk Threshold	Documented evidence the organization has a defined risk threshold.	RSK-01.1 RSK-01.3
181	E-RSK-07	Risk Management	Risk Tolerance	Documented evidence the organization has a defined risk tolerance.	RSK-01.1 RSK-01.4
182	E-RSK-08	Risk Management	Risk Appetite	Documented evidence the organization has a defined risk appetite.	RSK-01.1 RSK-01.5
183	E-RSK-09	Risk Management	Risk Catalog	Documented evidence of a risk catalog.	RSK-03.1
184	E-RSK-14	Risk Management	Risk Treatment Plan	Documented Risk Treatment Plan (RTP) for applicable stakeholders to utilize in remediating identified risks according to a defined timeline.	RSK-06.4
185	E-TDA-01	Technology Design & Acquisition	Secure Software Development Principles (SSDP)	Documented evidence of a Secure Software Development Principles (SSDP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	SEA-01 TDA-01 TDA-14 TDA-14.1 TDA-14.2
186	E-TDA-02	Technology Design & Acquisition	Secure Engineering & Data Privacy (SEDP)	Documented evidence of a Secure Engineering & Data Privacy (SEDP) program. This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	SEA-01 TDA-01 TDA-14 TDA-14.1 TDA-14.2
187	E-TDA-03	Technology Design & Acquisition	Application Security Testing (AST)	Documented evidence of application security testing (e.g., DAST, SAST, fuzzing, etc.).	TDA-06.2 TDA-09 TDA-09.1 TDA-09.2 TDA-09.3 TDA-09.4 TDA-09.5 TDA-09.6
188	E-TDA-04	Technology Design & Acquisition	Design and Development Plan (DDP)	Documented evidence of an engineering method to control the design process and govern the lifecycle of the product/service.	SEA-01 SEA-02 SEA-03 TDA-02.3 TDA-05 TDA-06.3

					TDA-14 TDA-14.1 TDA-14.2
189	E-TDA-05	Technology Design & Acquisition	Failure Mode and Effect Analysis (FMEA)	Documented evidence of an engineering method designed to define, identify and present solutions for system failures, problems, or errors.	TDA-01.1 TDA-06.5 TDA-09
190	E-TDA-06	Technology Design & Acquisition	Multi Patient Harm View (MPHV)	Documented evidence of a description of a Multi Patient Harm View (MPHV) that explains how the device / system defends against and/or responds to attacks with the potential to harm multiple patients. *[note MPHV is specific to medical device manufacturers]*	TDA-01.1 TDA-02 TDA-04 TDA-04.1
191	E-TDA-07	Technology Design & Acquisition	Ports, Protocols & Services (PPS)	Documented evidence of all ports, protocols and services in use by the system, application or service.	TDA-01.1 TDA-02.1 TDA-02.5 TPM-04.2
192	E-TDA-08	Technology Design & Acquisition	Secure Engineering Principles (SEP)	Documented evidence of defined secure engineering principles used to ensure Sensitivity, Integrity, Availability & Safety (CIAS) concerns are properly addressed in the design and implementation of Technology Assets, Applications and/or Services (TAAS).	SEA-01 TDA-01 TDA-06 TDA-14 TDA-14.1 TDA-14.2
193	E-TDA-09	Technology Design & Acquisition	Security Architecture View	Documented evidence that identifies security-relevant system elements and their interfaces: • Define security context, domains, boundaries and external interfaces of the system; • Align the architecture with (a) the system security objectives and requirements, (b) security design characteristics; and • Establish traceability of architecture elements to user and system security requirements.	CLD-02 SEA-01 SEA-02 SEA-03
194	E-TDA-10	Technology Design & Acquisition	Security Use Case View (SUCV)	Documented evidence of diagrams, with explanatory text, describing various security scenarios in each of the operational and clinical functionality states of the system and how the system addresses each scenario architecturally. *[note SUCV is specific to medical device manufacturers]*	TDA-04 TDA-04.1 TDA-06.2

195	E-TDA-11	Technology Design & Acquisition	Software Assurance Maturity Model (SAMM)	Documented evidence of a Software Assurance Maturity Model (SAMM).	TDA-06 TDA-06.3
196	E-TDA-12	Technology Design & Acquisition	Software Bill of Materials (SBOM)	Documented evidence of a Software Bill of Materials (SBOM).	TDA-04.2
197	E-TDA-14	Technology Design & Acquisition	System Security Plan (SSP)	Documented evidence of at least one (1) System Security Plan (SSP) that covers the sensitive/regulated data environment. There may be multiple SSPs, based on applicable contracts.	AST-02.4 IAO-03
198	E-TDA-15	Technology Design & Acquisition	Updateability / Patchability View	Documented evidence of a description of the end-to-end process permitting software updates and patches to be deployed to the device/service.	TDA-01.1 TDA-01.2 TDA-04.1
199	E-TDA-17	Technology Design & Acquisition	System Design Documentation	Documented evidence of system design documentation.	TDA-01 TDA-01.1
200	E-THR-03	Threat Management	Threat Intelligence Feeds (TIF)	Documented evidence of threat intelligence feeds.	THR-03
201	E-THR-04	Threat Management	Threat Intelligence Program (TIP)	Documented evidence of a formal capability that intakes and analysis threat information to determine specific threat to the organization and necessary actions to mitigate the threat(s).	THR-01 THR-04 THR-05
202	E-THR-05	Threat Management	Threat Mitigation	Documented evidence of steps taken to mitigate identified threats.	TDA-06.2 THR-07 VPM-01 VPM-04
203	E-THR-06	Threat Management	Threat Catalog	Documented evidence of a threat catalog.	THR-09
204	E-THR-07	Threat Management	Threat Analysis	Documented evidence of a completed threat analysis.	THR-10

205	E-TPM-01	Third-Party Management	Third-Party Contracts	Documented evidence of third-party contractual obligations for cybersecurity & data privacy protections.	PRI-07 PRI-07.1 PRI-07.2 TPM-01 TPM-03.2 TPM-03.3 TPM-04.1 TPM-05 TPM-04.3 TPM-05.3 TPM-05.6 TPM-06 TPM-10 TPM-11
206	E-TPM-02	Third-Party Management	Third-Party Criticality Assessment	Documented evidence of third-party criticality assessment that evaluates the critical nature of each third-party the organization works with.	RSK-02 RSK-02.1 TDA-06.1 TPM-02 TPM-03.2 TPM-03.3 TPM-04.1
207	E-TPM-03	Third-Party Management	Third-Party Service Reviews	Documented evidence of a formal, annual stakeholder review of third-party services for each External Service Provider (ESP).	TPM-01 TPM-03.2 TPM-03.3 TPM-04.1 TPM-05 TPM-05.5 TPM-08 TPM-09
208	E-TPM-04	Third-Party Management	Service Level Agreements (SLAs)	Documented evidence of third-party Service Level Agreements (SLAs) to support business operations.	BCD-09.3 BCD-10.1 OPS-03
209	E-TPM-05	Third-Party Management	Break Clauses	Documented evidence of "break clauses" in third-party contracts.	TPM-03.2 TPM-03.3 TPM-05.7
210	E-TPM-06	Third-Party Management	Third-Party Terms & Conditions	Documented evidence of terms and conditions for external systems.	TPM-01 TPM-05
211	E-TPM-07	Third-Party Management	System Connection or Processing Agreements	Documented evidence of system connection or processing agreements.	TPM-05

212	E-VPM-01	Vulnerability & Patch Management	Vulnerability & Patch Management Program (VPMP)	Documented evidence of a Vulnerability & Patch Management Program (VPMP). This is program-level documentation in the form of a runbook, playbook or a similar format provides guidance on organizational practices that support existing policies and standards.	VPM-01 VPM-02 VPM-03
213	E-VPM-05	Vulnerability Management	Vulnerability Assessments	Documented evidence of internal and external vulnerability assessment activities.	VPM-06 VPM-06.6 VPM-06.7
214	E-VPM-09	Vulnerability Management	Flaw Remediation Actions	Documented evidence of list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes and other software updates to correct system flaws).	VPM-02
215	E-VPM-10	Vulnerability Management	Applicable Flaws & Vulnerabilities	Documented evidence of flaws and vulnerabilities potentially affecting a specific system, application and/or service.	VPM-03 VPM-05
216	E-VPM-11	Vulnerability Management	Vulnerability Scanning	Documented evidence of internal and external vulnerability scans being performed.	VPM-06

217	E-END-01	Endpoint Security	Endpoint Security Tools	Documented evidence of endpoint security tools employed by the organization to ensure secure, compliant and resilient Technology Assets, Applications and/or Services (TAAS) (e.g., antimalware, FIM, etc.).	END-01
					END-04
					END-06

218	E-END-03	Endpoint Security	Antimalware Scanning Results	Documented evidence of scan results from malicious code protection mechanisms.	END-04.3 MON-01.4