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

START HERE

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

- 1a — GOV-08 — Define the entity's mission to establish the business context for necessary SCR capabilities.
- 1b — GOV-01, GOV-01.1, GOV-04, GOV-04.1 — Establish a **Security, Compliance & Resilience Program (SCRP)**, including enforcement & resourcing authority.
- 1c — CPL-01, GOV-15.1 — Define **Minimum Compliance Requirements (MCR)** that reflect the entity's applicable statutory, regulatory and contractual obligations for cybersecurity and data protection.
- 1d — GOV-15.1, RSK-03.1, THR-09 — Define preliminary **Discretionary Requirements** that reflect the entity's reasonable security and resilience expectations, based on applicable threats and risks (e.g., risk & threat catalogs).
- 1e — GOV-15, GOV-15.1 — Define the preliminary **Living Control Set (LCS)** for the entity, based on OSR and MCR. This is the **Minimum Security Requirements (MSR)** baseline.
- 1f — CPL-01.2 — Define the scope of the SCRP, based on the LCS and applicable **People, Processes, Technology, Data & Facilities (PPTDF)**.
- 1g — PRM-01.2 — Define target maturity criteria at the domain or control level for the LCS.

SCRMS Principle #1: Establish Context · SCRMS Principle #2: Identify Applicable Controls · SCRMS Principle #3: Define Maturity Expectations

2 Implement Centralized Governance Practices

- 2a — GOV-02 — From a centralized authority, develop, implement and maintain policies and standards to address SCRP needs, based on the LCS.
- 2b — GOV-02.1 — Provide the capability to manage exception requests to published standards.
- 2c — GOV-01.2, GOV-01.3 — Provide a commitment to continuously improve security, compliance & resilience capabilities.
- 2d — AST-01.2, GOV-15.2, OPS-01.1 — Identify stakeholders and assign control ownership from the LCS to applicable stakeholders. Stakeholders develop and maintain **Standardized Operating Procedures (SOP)** to implement controls.

SCRMS Principle #4: Publish Governance Documentation · SCRMS Principle #5: Assign Stakeholder Accountability

3 Align Risk Management Practices Across The Entity

- 3a — RSK-01 — Develop & implement an entity-wide **Risk Management Program (RMP)** for SCRP operations to identify, assess and remediate risk that is tied into **Enterprise Risk Management (ERM)** practices.
- 3b — RSK-01.3, RSK-01.4, RSK-01.5 — Define entity-specific risk appetite, risk threshold and risk tolerance criteria.
- 3c — GOV-15.1, GOV-15.2, GOV-16.1, GOV-16.2 — Define materiality for the entity, UNLESS that criteria to define material controls, material incidents, material threats and material risks.
- 3d — RSK-01.1, RSK-03, RSK-04, RSK-04.1, RSK-04.2, RSK-05 — Define a risk assessment methodology that is appropriate for the entity's SCRP needs to identify, categorize and assess risks.
- 3e — RSK-06 — Define stakeholder requirements for risk remediation actions to remediate risks to an acceptable level.
- 3e — RSK-04.1, IAO-05 — Develop a centralized risk register or **Plan of Action & Milestones (POA&M)** to provide situational awareness of risks and govern remediation activities.

4 Gain Clarity On The Entity's PPTDF

- 4a — AST-02 — Create and maintain a detailed inventory for all **Technology Assets, Applications, Services and/or Data (TAASD)**.
- 4b — TPM-01.1 — Create and maintain a detailed inventory for all **External Service Providers (ESP)** and **Cloud Service Providers (CSP)**.
- 4c — CLD-09, DCH-00.2, DCH-19, DCH-24, PRM-05.4, PRM-09.4 — Create and maintain a detailed inventory for all sensitive and/or regulated data, including geolocation information.
- 4d — AST-04 — Create detailed network diagrams that cover all **Technology Assets, Applications and/or Services (TAAS)**, including TAAS maintained by ESP and/or CSP.
- 4e — AST-02.8, AST-04 — Create **Data Flow Diagrams (DFD)** that shows how sensitive and/or regulated data flows across the entity's TAAS, including contractor flow-down.
- 4f — BCD-02, TPM-02 — Identify critical TAAS, including ESP and CSP.
- 4f — BCD-01.4 — 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.

5 Resource The SCRP

- 5a — PRM-02, PRM-01.1, PRM-03 — Develop & implement a resource plan (e.g., business plan, budget, road map, etc.) to operationalize the entity's SCRP (e.g., necessary PPTDF components).
- 5b — PRM-01, PRM-01.1, PRM-03, PRM-04, PRM-05 — Prioritize stakeholder objectives based on the resource plan for PPTDF.

SCRMS Principle #6: Prioritize Capability According To Risk

6 Establish Criteria To Be Secure, Compliant & Resilient

- 6a — SEA-01, SEA-01.2, SEA-01.3, SEA-02, SEA-02.3, SEA-03, SEA-20 — Secure engineering principles are defined to ensure security, compliance & resilience capabilities are implemented by default and by design.
- 6b — PRM-05, PRM-07 — Stakeholders govern security, compliance & resilience requirements across the **System Development Lifecycle (SDLC)**.
- 6c — TDA-01, TDA-01.1, TDA-02, TDA-02.1, TDA-02.10, TDA-04.2, TDA-05, TDA-06, TDA-06.1, TDA-06.2, TDA-06.3, TDA-07, TDA-09 — Security, compliance & resilience capabilities are implemented by default and by design in product management processes (e.g., updates, features, etc.)
- 6d — CAP-01, CAP-03, CAP-05 — Implement a capacity and performance management capability to support resilience requirements.
- 6e — GOV-15.3, GOV-15.4, IAO-01, IAO-02, IAO-02.4, IAO-03, IAO-04, IAO-05, IAO-06 — Implement an **Information Assurance Program (IAP)** to ensure secure, compliant & resilient capabilities are included by default and by design.
- 6f — RSK-06.1, RSK-06.2, RSK-06.4 — Implement **Risk Treatment Plans (RTP)** that include viable compensating controls when primary controls cannot be implemented or are deficient.

7 Establish Capabilities To Secure The Supply Chain

- 7a — RSK-09, TPM-03 — Develop a **Cybersecurity Supply Chain Risk Management (C-SCRM) Plan** that is applicable across the entity.
- 7b — TPM-01, TPM-03, TPM-04 — Develop and implement acquisition strategies, contract tools, and procurement methods to operationalize the C-SCRM Plan.
- 7c — TPM-05, TPM-05.2, TPM-05.7 — Enforce C-SCRM requirements across the supply chain through contracts and flow-down requirements.
- 7d — RSK-09.1, TPM-04.1 — Establish a process for identifying and addressing weaknesses or deficiencies in the supply chain elements and processes.
- 7e — TPM-05.4 — Create a **Responsible, Accountable, Supportive, Consulted & Informed (RASIC)** matrix to eliminate assumptions with ESP.

8 — OPS-01, OPS-02, OPS-03 — Empower cybersecurity and data protection personnel to enforce secure, compliant and resilient practices. POA&M deficiencies.

9 — HRS-01, HRS-01.1, HRS-02, HRS-02.1, HRS-04, HRS-04.1, HRS-05, HRS-05.1, HRS-05.7, HRS-07, HRS-07.1, HRS-08, HRS-09, HRS-10, HRS-13, HRS-14 — Work with **Human Resources (HR)** to ensure personnel security requirements are integrated into HR operations. POA&M deficiencies.

10 — DCH-01, DCH-01.1, DCH-01.4, DCH-02, DCH-13, DCH-13.3, DCH-17, DCH-18, DCH-19, DCH-21, DCH-24, DCH-25 — Define and implement 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.

11 — CLD-01, CLD-02, CLD-09, CLD-10, NET-02, NET-02.2, NET-03, NET-04, NET-04.1, NET-10, NET-12, NET-12.2, NET-14, NET-14.5, NET-14.7, NET-16, NET-18, WEB-01, WEB-10 — Develop and implement a segmented network architecture and industry-recognized secure practices for networking. POA&M deficiencies.

12 — CHG-01, CHG-02, CHG-02.1, CHG-03 — Develop & implement change control processes, including a **Change Control Board (CCB)**. POA&M deficiencies.

13 — IRO-02, IRO-02, IRO-10, IRO-04, IRO-07, IRO-10, IRO-13 — Develop & implement incident response capabilities to detect, respond and recover from incidents. POA&M deficiencies.

14 — MON-01, MON-01.2, MON-01.4, MON-01.8, MON-03, MON-11.3, MON-16, THR-03 — Develop & implement situational awareness capabilities through threat intelligence, log collection and analysis (e.g., SIEM). POA&M deficiencies.

15 — CFG-01, CFG-02, CFG-02.7, CFG-03, CRY-01, CRY-03, CRY-05, CRY-06, CRY-09 — Identify, build & implement **Secure Baseline Configurations (SBC's)** (e.g., hardening standards) for all technology platforms and enforcing secure configurations (e.g., Directory Services, Active Directory, Intune, etc.). POA&M deficiencies.

16 — IAC-01, IAC-01.2, IAC-01.3, IAC-06, IAC-07, IAC-08, IAC-10, IAC-10.8, IAC-10.11, IAC-15, IAC-15.7, IAC-16, IAC-16.1, IAC-17, IAC-20, IAC-21 — Develop & implement **Identity & Access Management (IAM)** capabilities to address "least privilege" and **Role-Based Access Control (RBAC)**. POA&M deficiencies.

17 — AST-01, AST-01.1, AST-01.2, AST-02, AST-02.8, AST-04, AST-09, AST-16, END-01, END-04, END-04.4, END-04.7, END-08, MDM-01, MDM-03, MDM-05, MDM-06, MDM-07, MDM-11 — Develop & implement **Information Technology Asset Management (ITAM)** practices, including **Endpoint Device Management (EDM)**. POA&M deficiencies.

18 — EMB-01, EMB-02, EMB-07, EMB-10 — Develop & implement embedded technology capabilities for **Operational Technology (OT)** and **Internet of Things (IoT)** assets. POA&M deficiencies.

19 — MNT-01, MNT-02, MNT-05 — Develop & implement proactive maintenance practices. POA&M deficiencies.

20 — VPM-01, VPM-02, VPM-03, VPM-05, VPM-06 — Develop & implement **Attack Surface Management (ASM)** practices. POA&M deficiencies.

21 — AAT-01, AAT-01.2, AAT-02, AAT-02.3, AAT-10 — Develop & implement **Artificial Intelligence & Autonomous Technologies (AAT)** governance practices. POA&M deficiencies.

22 — BCD-01, BCD-01.4, BCD-01.5, BCD-02, BCD-02.1, BCD-02.2, BCD-02.3, BCD-11, BCD-12 — Develop & implement **Business Continuity & Disaster Recovery (BCDR)** capabilities. POA&M deficiencies.

23 — PRI-01, PRI-01.11, PRI-02, PRI-03, PRI-04, PRI-05.5, PRI-06, PRI-14, PRI-17, RSK-10 — Develop & implement a data privacy program. POA&M deficiencies.

24 — PES-01, PES-01.1, PES-01.2, PES-02, PES-02.1, PES-03, PES-04, PES-05, PES-06, PES-12 — Develop & implement physical & environmental security capabilities. POA&M deficiencies.

25 — SAT-01, SAT-02, SAT-03 — Build and maintain a security minded workforce through security, compliance & resilience training & awareness. POA&M deficiencies.

26 — THR-01, THR-03, THR-09, THR-10 — Build and maintain a **Threat Intelligence Program (TIP)**. POA&M deficiencies.

27 — GOV-15.5, GOV-19, GOV-19, CPL-01.1, CPL-01.3, CPL-01.4, CPL-02.2, CPL-03.2 — Provide oversight of SCRP controls, including deficiencies and remediation activities.

SCRMS Principle #7: Maintain Situational Awareness

28 — CPL-01.1, IAO-01, RSK-04.1, TPM-05.5, TPM-08, TPM-10 — Manage changes that affect the entity's security, compliance & resilience, including the supply chain.

SCRMS Principle #8: Manage Risk

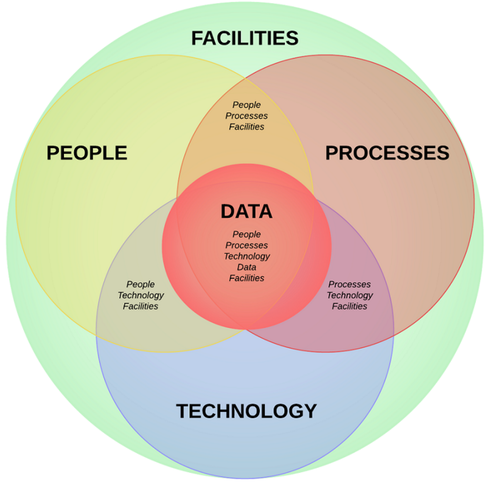
29 — BCD-04, IRO-06 — Test processes to ensure they are secure, compliant and resilient.

30 — GOV-01.2, GOV-01.3, GOV-05, GOV-06.1, GOV-05.2 — Report the status of the SCRP to a governing body (e.g., quarterly business reviews to a steering committee).

SCRMS Principle #9: Evolve Processes

LEGEND

- Applicable SCF Control
- Due Diligence Focus
- Due Care Focus



PRIORITIZED IMPLEMENTATION GUIDE

SCF SCRMS

version 2026.1

Copyright © 2026 by Secure Controls Framework Council, LLC (SCF Council). All rights reserved.

All text, images, logos, trademarks and information contained in this document are the intellectual property of SCF Council, unless otherwise indicated. Modification of any content, including text and images, requires the prior written permission of SCF Council. Requests may be sent to support@securecontrolsframework.com.