

Supply Chain Risk Management (SCRM) Plan

Version:

{Version Number}

Date:

{Version Date}

Document Template Version History

This document is required to be fully populated for all StateRAMP Baselines.

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description | Version | Author |
| 12/01/2023 | Original publication.  Based on NIST SP 800-161, Appendix D | 1.0 | StateRAMP |

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description | Version | Author |
| {Version Date} | {Change Description/Initial Publication} | {Document Version Number} |  |

Prepared by

|  |  |
| --- | --- |
| Identification of Organization that Prepared this Document | |
| **Organization Name** | <Enter Company/Organization>. |
| **Street Address** | Click here to enter text. |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State, Zip** | <Enter Zip Code> |

Prepared for

|  |  |
| --- | --- |
| Identification of Organization that Prepared this Document | |
| **Organization Name** | <Enter Company/Organization>. |
| **Street Address** | Click here to enter text. |
| **Suite/Room/Building** | <Enter Suite/Room/Building> |
| **City, State, Zip** | <Enter Zip Code> |

TABLE OF CONTENTS

[1 Introduction 0](#_Toc152321403)

[2 Purpose 0](#_Toc152321404)

[3 Scope 1](#_Toc152321405)

[4 Related Laws, Regulations, and Policies 2](#_Toc152321406)

[5 SCRM Strategy and Implementation Plan 3](#_Toc152321407)

[5.1 Authority and Compliance 3](#_Toc152321408)

[5.2 Strategic Objectives 3](#_Toc152321409)

[5.3 Roles and Responsibilities 5](#_Toc152321410)

[5.4 Definitions 5](#_Toc152321411)

[6 SCRM Plan 5](#_Toc152321412)

[6.1 System Information 5](#_Toc152321413)

[6.2 System Operational Status 9](#_Toc152321414)

[6.3 System/Network Diagrams, Inventory, and Life Cycle Activities 9](#_Toc152321415)

[6.4 Information Exchange and System connections 9](#_Toc152321416)

[6.5 Security Control Details 9](#_Toc152321417)

[6.6 Role Identification 10](#_Toc152321418)

[6.7 Contingencies and Emergencies 11](#_Toc152321419)

[7 Cybersecurity Supply Chain Risk Assessment Process 12](#_Toc152321420)

[7.1 SCRM Process 12](#_Toc152321421)

[8 Acronym List 17](#_Toc152321422)

[9 Attachments 18](#_Toc152321423)

# Introduction

To address cybersecurity risks throughout the supply chain, enterprises develop a Cybersecurity Supply Chain Risk Management (SCRM) strategy. The SCRM strategy, accompanied by an implementation plan, is at the organization level (Level 1), though different mission and business areas (Level 2) may further tailor the SCRM strategy to address specific mission and business needs, as outlined at the organization level. Organizations may layer additional tailoring at the system level (Level 3). Further information regarding Cybersecurity Supply Chain Risk Management (SCRM) strategy can be found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161.

The SCRM strategy and implementation plan should anchor to the overarching enterprise risk management strategy and comply with applicable laws, executive orders, directives, and regulations. Typical components of the strategy and implementation plan, as outlined in the below template, include strategic approaches to reducing an enterprise’s supply chain risk exposure via enterprise-wide risk management requirements, ownership, risk tolerance, roles and responsibilities, and escalation criteria. Note that the strategy and implementation plan may be developed as a single document or split apart into multiple documents. In any case, these SCRM outputs should be closely related in nature.

# Purpose

The purpose of this document is to provide a strategic roadmap for implementing effective SCRM capabilities, practices, processes, and tools within the enterprise in support of its vision, mission, and values.

The approach is organized around a set of objectives that span the scope of the enterprise’s mission and reflect a phased, achievable, strategic approach to ensuring the successful implementation and effectiveness of SCRM efforts across the enterprise.

This document discusses the necessary core functions, roles, responsibilities, and the approach that the enterprise will take to implement SCRM capabilities within the enterprise. As mission and business policies and system plans are developed and completed, they will be incorporated as attachments to this document. All three tiers of documentation should be periodically reviewed together to ensure cohesion and consistency.

The focus of this strategy and implementation plan is intentionally targeted at establishing a core foundational capability. These baseline functions – such as defining policies, ownership, and dedicated resources – will ensure that the enterprise can expand and mature its SCRM capabilities over time. This plan also acknowledges and emphasizes the need to raise awareness among staff and ensure proper training in order to understand SCRM and grow the competencies necessary to be able to perform SCRM functions.

This initial strategy and implementation plan also recognizes dependencies on industry-wide coordination efforts, processes, and decisions. As government and industry-wide direction, process guidance, and requirements are clarified and communicated, the enterprise will update and refine its strategy and operational implementation plans and actions.

# Scope

The scope of this appendix is to outline the enterprise’s high-level purpose for the strategy and implementation document, aligning that purpose with the enterprise’s mission, vision, and values. Describe where the strategy and implementation document reside relative to other SCRM documentation that must be maintained at various levels. Provide clear direction around the enterprise’s SCRM priorities and its general approach for achieving those priorities.

# Related Laws, Regulations, and Policies

The enterprise should ensure that SCRM plan controls are consistent with applicable statutory authority, regulatory requirements and external guidance, publications promulgated by the National Institute of Standards and Technology (NIST); and internal SCRM policies and strategy documents.

**The following references apply:**

* NIST SP 800‐53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations
* Committee on National Security Systems. CNSSD No. 505. (U) Supply Chain Risk Management (SCRM)
* NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
* NIST SP 800‐161, Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
* OMB Circular A‐130 Managing Information as a Strategic Resource
* Federal Acquisition Supply Chain Security Act of 2018
* Executive Order 14028 of May 12, 2021, Improving the Nation’s Cybersecurity

# SCRM Strategy and Implementation Plan

## Authority and Compliance

The following laws, executive orders, directives, regulations, policies, standards, and guidelines that govern SCRM Strategy and Implementation are listed below:

**Legislation:**

* Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018
* Federal Information Security Modernization Act of 2014
* Section 889 of the 2019 National Defense Authorization Act – “Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment”
* Gramm-Leach-Bliley Act
* Health Insurance Portability and Accountability Act
* Executive Order 14028 of May 12, 2021, Improving the Nation’s Cybersecurity

**Regulations:**

* NYDFS 23 NYCRR 500: Section 500.11 Third Party Service Provider Security Policy
* CIP-013-1: Cyber Security – Supply Chain Risk Management
* FFIEC Information Security Handbook II.C.20: Oversight of Third-Party Service Providers

**Guidelines:**

* NIST 800-53, Revision 5: CA-5, SR-1, SR-2, SR-3
* NIST SP 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
* NIST 800-37, Revision 2
* NIST 800-161, Revision 1: Appendix C
* ISO 28000:2007

## Strategic Objectives

Strategic objectives establish the foundation for determining enterprise-level SCRM controls and requirements. Each objective supports achievement of the enterprise’s stated purpose in pursuing sound SCRM practices and risk-reducing outcomes. Together, the objectives provide the enterprise with the essential elements needed to bring SCRM capabilities to life, and effectively pursue the enterprise’s purpose.

In aggregate, strategic objectives should address essential SCRM capabilities and enablers,

such as:

* Implementing a risk management hierarchy and risk management approach
* Establishing an enterprise governance structure that integrates SCRM requirements and incorporates these requirements into enterprise policies
* Defining a supplier risk assessment approach
* Implementing a quality and reliability program that includes quality assurance and quality control processes and practices
* Establishing explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security (and other relevant) functions
* Ensuring that adequate resources are dedicated and allocated to information security and SCRM to ensure the proper implementation of policy, guidance, and controls
* Implementing a robust incident management program to successfully identify, respond to, and mitigate security incidents
* Including critical suppliers in contingency planning, incident response, and disaster recovery planning and testing

### Objective 1: Effectively manage cybersecurity risks throughout the supply chain

This objective addresses the primary intent of the enterprise’s pursuit of SCRM. Establishing and sustaining an enterprise-wide SCRM program will enable the enterprise’s risk owners to identify, assess, and mitigate supply chain risk to the enterprise’s assets, functions, and associated services. Implementing an initial capability that can sustain and grow in scope of focus, breadth, and depth of function will be done in phases and will incorporate holistic “people, process, and technology” needs to ensure that the enterprise is able to achieve desired SCRM goals in areas such as improving enterprise awareness, protection, and resilience.

### Objective 2: Serve as a trusted source of supply for customers

Addressing customer supply chain risks at scale and across the enterprise’s diverse portfolio demands a prioritization approach, structure, improved processes, and ongoing governance. SCRM practices and controls need to be tailored to address the distinct and varied supply chain threats and vulnerabilities that are applicable to the enterprise’s customers. This objective can be achieved by:

* Strengthening vetting processes, SCRM requirements, and oversight of external providers and
* Ensuring that customer needs are met in line with their cybersecurity risk appetite, tolerance, and environment

### Objective 3: Position the enterprise as an industry leader in SCRM

The enterprise is well-positioned to enable and drive forward improvements that address how cybersecurity risk is managed in supply chains across the industry. Therefore, the enterprise must use this position to advocate for communication, incentivization, and the education of industry players about the enterprise’s requirements and expectations related to addressing supply chain risk.

## Roles and Responsibilities

Designate those responsible for the Strategy and Implementation template, as well as its key contributors. Include the role and name of each individual or group, as well contact information where necessary (e.g., enterprise affiliation, address, email address, and phone number).

**Senior leadership shall:**

* Endorse the enterprise’s SCRM strategic objectives and implementation plan,
* Provide oversight of SCRM implementation and effectiveness,
* Communicate SCRM direction and decisions for priorities and resourcing needs,
* Determine the enterprise’s risk appetite and risk tolerance, and
* Respond to high-risk SCRM issue escalations that could impact the enterprise’s risk posture in a timely manner.

**Mission and business owners shall:**

* Determine mission-level risk appetite and tolerance, ensuring that they are in line with enterprise expectations;
* Define supply chain risk management requirements and the implementation of controls that support enterprise objectives;
* Maintain criticality analyses of mission functions and assets; and
* Perform risk assessments for mission and business-related procurements.

## Definitions

* Enterprise: An organization with a defined mission, goal, and boundary that uses information systems to execute that mission and has the responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information, and mission management. In most cases this is a reference to {Service Provider Organization} .
* Objective: An enterprise’s broad expression of goals and a specified target outcome for operations.

# SCRM Plan

## System Information

### System Name and Identifier

|  |  |
| --- | --- |
| System Information | |
| **Service Provider Name:** | {Service Provider Organization} |
| **Product Name:** | {Product Name} |
| **StateRAMP Package ID:** | {StateRAMP Package ID} |

This SCRM plan provides an overview of the security requirements for {Service Provider Organization} {Product Name} and describes the supply chain cybersecurity controls in place or planned for implementation to provide fit-for-purpose SCRM controls that are appropriate for the information to be transmitted, processed, or stored by the system.

The security safeguards implemented for {Product Name} meet the requirements set forth in the enterprise’s SCRM strategy and policy guidance.

## System Description

{Insert System Description for Service Offering}

## System Operational Status

**Table 6.3: System Operational Status**

|  |  |  |
| --- | --- | --- |
| System Status | | |
|  | Operational | The system is currently operating and is in production |
|  | Under Development | The system is being designed, developed, or implemented |
|  | Major Modification | The system is undergoing a major change, development, or transition |
|  | Disposition | The system is no longer operational. |

## System/Network Diagrams, Inventory, and Life Cycle Activities

Current and detailed system and network diagram and system component inventory information can be found in the System Security Plan for {Product Name}.

## Information Exchange and System connections

A list any information exchange agreements (e.g., Interconnection Security Agreements (ISA), Memoranda of Understanding (MOU), Memoranda of Agreement (MOA)) between the system and another system, the date of the agreement, the security authorization status of the other systems, the name of the authorizing official, a description of the connection, and diagrams that show the flow of any information exchange can be found in the System Security Plan for {Product Name}.

## Security Control Details

Please refer to the *Supply Chain Risk Management* section of the *{Service Provider Organization} {Product Name} System Security Plan (SSP)* for a list of applicable StateRAMP Supply Chain Risk Management controls and their associated implementation details for {Product Name}.

SR‐6 SUPPLIER ASSESSMENTS AND REVIEWS

**Implementation:** As a part of a comprehensive, defense‐in‐breadth information security strategy, the enterprise established a SCRM program to address the management of cybersecurity risks throughout the supply chain. The {SCRA Review Team} is responsible for conducting assessments of cybersecurity risks that arise from business partners seeking to integrate with {Product Name} in accordance with enterprise‐wide SCRM policy requirements.

Additionally, SA-12 Control Enhancements (2), (7) and (8) from NIST SP 800-53r4 are =applicable.

SA-12 (2) SUPPLIER REVIEWS

[NIST SP 800-53r5 Status: Withdrawn: Moved to SR-6.]

**Implementation:** The {SCRA Review Team} provides supplier reviews to business partners in the form of Supply Chain Risk Assessments (SCRAs) before entering into a contractual agreement to acquire information systems, components, or services in relation to {Product Name}. The assessment may include reviewing the supplier’s SSP, their SOC2 report, or other relevant security documentation. In the event the supplier does not have a security package available for review, {Service Provider Organization} request the supplier to complete the {Service Provider Organization} Vendor Security Questionnaire (VSQ).

SA-12 (7) ASSESSMENT PRIOR TO SELECTION/ACCEPTANCE/UPDATE

[NIST SP 800-53r5 Status: Withdrawn: Moved to SR-5(2).]

**Implementation:** The *{Service Provider Organization} Security Procedures, Supply Chain Risk Management* volume defines what {Product Name} activities require an Supply Chain Risk Assessment.

SA-12 (8) USE OF ALL‐SOURCE INTELLIGENCE

[NIST SP 800-53r5 Status: Withdrawn: Incorporated into RA-3(2).]

**Implementation:** The {SCRA Review Team} may utilize all‐source intelligence when conducting supply chain risk assessments for {Product Name}. This review may also include reviewing the suppliers SSP, their SOC2 report, responses to {Service Provider Organization} Vendor Security Questionnaire, or other relevant security documentation. In the event the supplier does not have a security package available for review, {Service Provider Organization} request the supplier to complete the {Service Provider Organization} Vendor Security Questionnaire (VSQ).

## Role Identification

Identify the role, name, department/division, primary phone number, and email address of key cybersecurity supply chain personnel or designate contacts (e.g., vendor contacts, acquisitions subject matter experts (SME), engineering leads, business partners, service providers) with a role, name, address, primary phone numbers, and email address.

**Table 6.4: SCRM Role Identification**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Department/Division | Primary Phone Number | Email Address |
| Purchasing Contact/SME |  |  |  |  |
| Software Admin |  |  |  |  |
| Legal Counsel |  |  |  |  |
| Product Requester |  |  |  |  |
| Information Security Reviewer |  |  |  |  |

## Contingencies and Emergencies

In the event of an emergency where equipment is urgently needed, the {SCRA Review Team} will offer its assistance through SCRM subject matter experts (SMEs) to provide help in the absence of formal tasking and chain of command approval. The CIO has the authority to provide such waivers to bypass normal procedures. The current contact information for SCRM SMEs is provided below:

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name | Phone Number | Email Address |
| SCRM SME POC |  |  |  |
| Alternate SCRM SME POC |  |  |  |
| Alternate SCRM SME POC |  |  |  |
| Acquisitions SME POC |  |  |  |
| Legal SME POC |  |  |  |

# Cybersecurity Supply Chain Risk Assessment Process

The Cybersecurity Supply Chain Risk Assessment (SCRA) guides the review of any third-party product, service, or supplier that could present a cybersecurity risk to a procurer. The objective of the SCRA process is to provide a toolbox of questions that an acquirer can choose to use or not use depending on the controls selected. Typically executed by SCRM PMOs at the operational level, the SCRASCRA considers available public and private information to perform a holistic assessment, including known cybersecurity risks throughout the supply chain, the likelihoods of their occurrence, and their potential impacts on an enterprise and its information and systems.

## SCRM Process

### Authority and Compliance

Legislation:

* Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018

Guidelines:

* NIST 800-53, Rev. 5: PM-30, RA-3, SA-15, SR-5
* NIST 800-37, Rev. 2
* NIST 800-161, Rev. 1: Appendix C
* ISO 28001:2007

### Description

The SCRA is intended to fairly and consistently evaluate risks posed to the enterprise via third parties that hold the potential for harm or compromise as a result of cybersecurity risks. Cybersecurity risk in the supply chain include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain, as well as the exposures, threats, and vulnerabilities to the supply chain and its suppliers.

The SCRA process provides tactical guidelines for the {Service Provider Organization} to review cybersecurity risk in the supply chain and ensure that SCRAs are appropriately, efficiently, and effectively carried out in line with enterprise mandates.

Requestors seeking to introduce third-party products, services, or suppliers into enterprise boundaries should familiarize themselves with the following process. This will ensure that requestors can provide the requisite information to the SCRA Review Team to ensure timely execution of SCRAs and are otherwise aligned with the steps of the SCRA.

To learn more about the SCRA process and/or submit an assessment request to {SCRA Review Team Name} Team, contact {SCRA Review Team email address/phone number/etc.}.

### Information Gathering and Scoping Analysis

The purpose of the Information Gathering and Scoping step is to gain key information to appropriately define the system, operations, supporting architecture, and boundaries and how they relate to {Service Provider Organization} regarding being integrated into our business systems and processes. Information gathered from this step should create a solid base of information to refer to during future steps, and to create a detailed understanding of the workings of the product or offering. It could also provide enough information to deny the request before moving onto future steps if the information gathered deems that appropriate.

A review of the vendor’s StateRAMP or FedRAMP status should be conducted. In the event that the vendor is not listed with either entity, {Service Provider Organization} SCRA Review Team may elect to review the vendor’s SOC2 report. If a SOC2 report is not available, the {Service Provider Organization} Vendor Security Questionnaire (VSQ) should be used for gathering information on the security practices and posture of the product, service, or supplier to be scoped and analyzed.

### Threat Analysis

The SCRA threat analysis evaluates and characterizes the level of threat to the integrity, trustworthiness, and authenticity of the product, service, or supplier as described below. This analysis is based on a threat actor’s capability and intent to compromise or exploit the product, service, or supplier being introduced into the supply chain.

To appropriately perform a threat analysis, SCRM PMOs and requestors should leverage the Vendor Security Questionnaire, located in *Section 9: Attachments* of this document, to coordinate the collection of information related to the product, service, or supplier’s operational details, ownership structure, key management personnel, financial information, business ventures, government restrictions, and potential threats. This information is analyzed and it is determined if possible threats toward {Service Provider Organization} would materialize if the product, service, or supplier were onboarded. Additional investigations of the aforementioned topics should be performed if red flags are observed during initial data collection.

### Vulnerability Analysis

Insert additional information, as appropriate, for your organization.

The SCRA vulnerability analysis evaluates and then characterizes the vulnerability of the product, service, or supplier throughout its life cycle and/or engagement. The analysis includes an assessment of the ease of exploitation by a threat actor with moderate capabilities. This analysis is based on a threat actor’s capability and intent to compromise or exploit the product, service, or supplier being introduced into the supply chain.

The {SCRA Review Team} and requestors should coordinate a discussion about the collected information related to the product, service, or supplier’s operational details, exploitability, service details, attributes of known vulnerabilities, and mitigation techniques. Through this discussion, the requestor would be informed of the findings, and potentially collect more information on how the product, service, or supplier is intended to be used with the {Service Provider Organization} organization.

### Impact Analysis

Insert additional information, as appropriate, for your organization.

The SCRA impact analysis evaluates and then characterizes the impact of the product, service, or supplier throughout its life cycle and/or engagement. The analysis includes an end-to-end functional review to identify critical functions and components based on an assessment of the potential harm caused by the probable loss, damage, or compromise of a product, material, or service to an enterprise’s operations or mission.

To appropriately perform an impact analysis, the {SCRA Review Team} and requestors should coordinate the collection of information related to the enterprise’s critical functions and components, the identification of the intended user environment for the product or service, and supplier information.

### Roles and Responsibilities

**The {SCRA Review Team} shall:**

* Maintain SCRA policies, procedures, and scoring methodologies;
* Perform SCRA standard operating procedures;
* Liaise with requestors seeking to procure a product, service, or supplier; and
* Report SCRA results to leadership to help inform enterprise risk posture.

**Each requestor shall:**

* Complete any SCRA request forms provided and provide all required information,
* Address any information follow-up requests from the {SCRA Review Team} resource completing the SCRA, and
* Adhere to any stipulations or mitigations mandated by the {SCRA Review Team} following approval of a SCRA request.

**Table 7‑1: SCRA Role Identification**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Role | Name | Department/Division | Primary Phone Number | Email Address |
| Information Security Reviewer |  |  |  |  |
| Information Security Reviewer |  |  |  |  |
| Information Security Reviewer |  |  |  |  |
| Information Security Review Approver |  |  |  |  |
| Information Security Review Approver |  |  |  |  |
| Chief Information Security Officer |  |  |  |  |
| SCRA  Requester |  |  |  |  |

### SCRM Process Flow

The diagram below represents a visualization of the overall SCRM process flow.

Insert diagram of the SCRM process, as appropriate, for your organization.

# Attachments

Reference any supporting documents, as appropriate.

|  |  |
| --- | --- |
| Document | Attached File Name |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |