



**TABLE OF
CONTENTS**

INTRODUCTION	1
SECURING YOUR ECOSYSTEM	2
SUPPLY CHAIN RISK ENVIRONMENT	3
THREAT LANDSCAPE	4
SUPPLY CHAIN RISKS	6
SUPPLY CHAIN SECURITY	9
FIXABLE OR FATAL?	10
KEY ORGANIZATIONAL COMPONENTS	12
RISK GOVERNANCE AND ACCOUNTABILITY	14
MANAGE SUPPLY CHAIN RISK	16
WHAT’S NEXT?	22
SCRM IMPLEMENTATION: ACTIONS AND OUTPUTS	23
EVALUATING YOUR ORGANIZATION’S SCRM PROGRAM	24
REFERENCES AND RESOURCES	25

INTRODUCTION

Global supply chains are an integral part of our world. Leveraging goods and services from across a global marketplace brings tremendous efficiencies to private sector entities, academic institutions, state and local governments, and federal departments and agencies. However, these same efficiencies also expose organizations to the risks from the global supply chain. The increased reliance on goods and services sourced from the global supply chain—and delivered through a digital infrastructure—allows an adversary to surveil, deny, disrupt, or otherwise degrade the critical control systems, services, and products that we depend on every day. Security-focused supply chain risk management (SCRM) programs provide an organization with

an enhanced view of its own risk exposure. Supply chain threats posed by sophisticated adversaries are often difficult to detect, which may expose organizations to unforeseen risks. Incorporating security principles—such as acquisition, cyber, and enterprise security—will provide additional information that an organization can use to better understand its overall risk posture. Further, this security-focused approach will assist organizations in tailoring mitigations to reduce supply chain risks.

This resource guide highlights SCRM policies, procedures, and best practices that can be integrated into an organization's overall risk management framework.



SECURING YOUR ECOSYSTEM

This document provides guidance on how to:



Understand your supply chain risk environment

- Supply chain threat landscape
- Acquisition life-cycle
- Supply chain security disciplines



Understand the key organizational components that contribute to effective SCRM activities

- Key business areas
- Stakeholder tiers for SCRM governance and accountability
- SCRM program roles and responsibilities
- SCRM program officials within your organization



Manage your supply chain risk

- Framing your risk
- Assessing the risk to your supply chain
- Responding to supply chain risk with appropriate mitigation strategies
- Monitoring the risk and improving your mitigation approaches

SUPPLY CHAIN RISK ENVIRONMENT

Supply chain risk is an important component of an organization's overall risk picture that requires careful consideration, both for economic interests and national security interests. Threats to the supply chain may materialize as the theft or loss of sensitive data, disruption of operations or services, insertion of malicious software or hardware, or any other compromise of an organization's systems or services.

Organizations' information communication technology and services (ICTS) are often the most critical assets in the organization. ICTS store and communicate sensitive organizational information and thus, they are "the key" to an organization's "crown jewels." Adversaries seek to exploit the inherent weaknesses in the ICTS supply chain a.k.a. "cyber supply chain" through the vulnerabilities in this critical supply chain. Furthermore, today's supply chain threats can originate from any source, ranging from nation-states and criminal organizations to lone wolves. Contemporary attackers can be well-funded

and organized, making them capable of using the cyber supply chain to clandestinely target organizations, corporate functions, their customers, and other critical information.

While adversaries often exploit the cyber supply chain, there are other threat vectors that organizations need to keep in mind when assessing overall risk. Organizations must guard against blended operations that may exploit legitimate means for illicit gains. Adversaries will use an organization's supply chain stakeholders - customers, suppliers, vendors, students, scientists, researchers, and corporate employees - to collect valuable data and information. Such supply chain exploitation, especially when executed in concert with cyber operations, threatens the integrity of key U.S. technology sectors, critical infrastructure, and the industrial base. Most organizational supply chain risks can be categorized into an acquisition, cyber, or enterprise risk, which are all part of developing an accurate picture of the supply chain risk environment.

THREAT LANDSCAPE

Adversarial control over ownership, legal environment, insider threats, physical intrusions, and technology dependencies present potential supply chain threat vectors.

THREATS

Supply chain threats target organizations from a number of threat vectors.



Adversarial Ownership

Suppliers, customers, or business partners may be owned, controlled, or influenced by an adversarial nation-state actor. Will this expose your organization's assets?



Cyber

Cyber threat actors may target your suppliers through cyber means to gain unauthorized access to your IT assets and systems. What is your supplier's cyber posture? Does it match yours?



Jurisdictional

Global suppliers must abide by the laws of the country in which they operate. Are those countries able to access your assets due to your supplier's global footprint?



Insider

Personnel security checks are in place to protect your employees and assets. But what controls are in place for a suppliers' employees?



Physical

Facility security protocols stop unauthorized access, destruction, or damage to employees and assets. How does your supplier mitigate these same physical vulnerabilities?



Technology

Employees and critical assets operate on IT. Could outdated technology expose your organization or your supplier's organization to vulnerabilities that adversaries could exploit?

To address these threats, Supply Chain Risk Management Programs need:

Acquisition Security, **C**yber Security, and **E**nterprise Security principles and best practices.

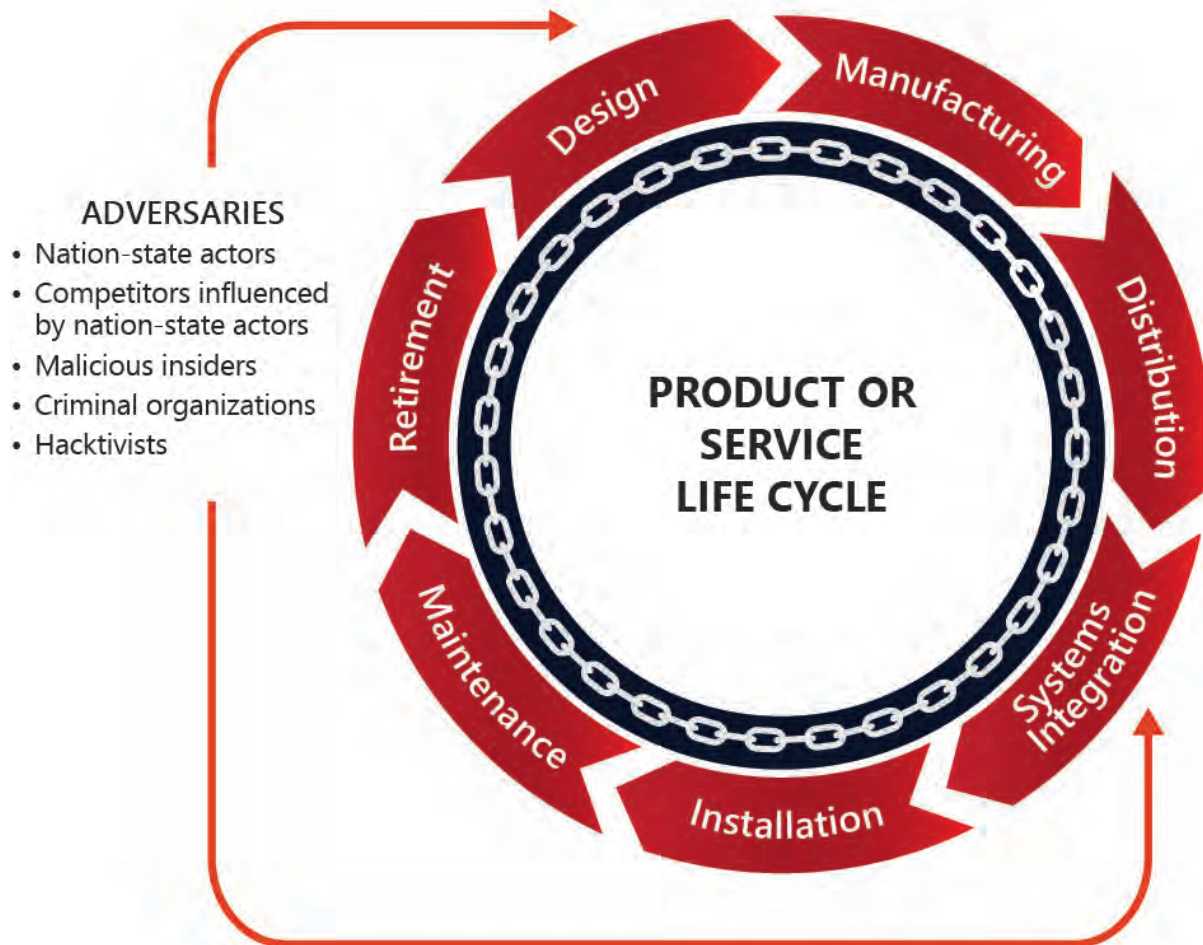


IMPACTS

If an adversary exploits access anywhere within the supply chain life cycle, impacts to your organization could include:

- Delayed or degraded production
- Lost intellectual property or competitive business advantage
- Compromised privacy or security
- Disruption of services
- Compromised information systems
- Exposed sensitive national security information
- Disrupted or degraded operations
- Legal or reputational impacts

METHODS AND POTENTIAL IMPACTS OF SUPPLY CHAIN ATTACKS

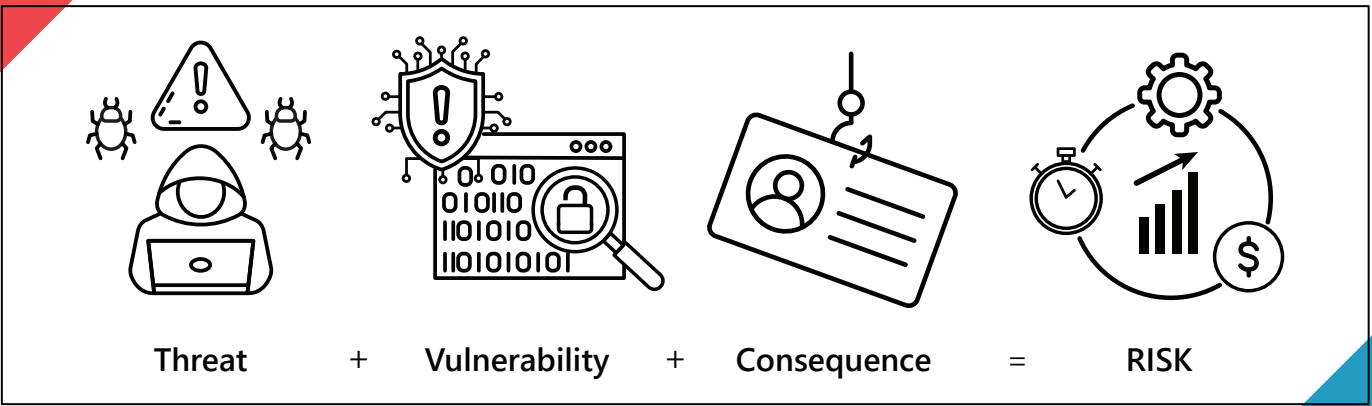


COMMON METHODS OF SUPPLY CHAIN ATTACKS

- Cyber compromise
- Theft/interdiction
- Sabotage
- Re-route
- Malicious component insertion
- Repair part compromise
- Trojan insertion/design to fail
- Fraud/counterfeit

SUPPLY CHAIN RISKS

An organization must understand the threat, vulnerability, and consequence of threat actors exploiting the supply chain threat vectors to understand the risks to an organization. This risk equation (threat + vulnerability + consequence = risk) is the foundation for building a SCRM program to address the ever-expanding supply chain threat landscape. Supply chain threats that operate through these vectors cause disruptions, shortages, delays, and added costs for essential commodities and services worldwide. Furthermore, supply chain threats from foreign adversarial exposure need to be included in the risk equation.



If not managed, the supply chain threats outlined above may present an acquisition risk, cyber risk, or enterprise risk to an organization.



ACQUISITION RISKS

Risks passed on from suppliers, vendors, investors, and customers that engage with an organization.



CYBER RISKS

Risks from cyber products and services that compromise the integrity of products and services.



ENTERPRISE RISKS

Risks from individuals with authorized access to an organization's information and assets.



ACQUISITION RISKS

Acquisition risks include a range of concerns, many of which are often inherent within the supply chain and derive from third-party sources, including corruption, infiltration, foreign influence, mergers, and intellectual property (IP) hacking or theft. Third-party risks, for example, refer to any potential risk that an organization faces due to external parties involved in its ecosystem or supply chain. These external parties may include vendors, suppliers, partners, contractors, or service providers who have been granted access to internal organizational data, infrastructure, operating systems, security measures, processes, or other sensitive information. Third parties introduce a wide variety of risk to an organization and mitigation plans must be in place to minimize consequences from such. Although some risks are generally unique to individual third parties, two main issues that can arise are loss of service for critical applications or services and loss of proprietary data, whether from customers, employees, or other third parties. Suppliers provide several avenues for attackers to access your network or data to disrupt your organization. Some methods to address risk may also include restricting access on certain vendors that operate from geographical regions identified as countries of concern, contract language, and cybersecurity requirements. Addressing risks also require organizations to conduct a full life-cycle review of an acquisition.

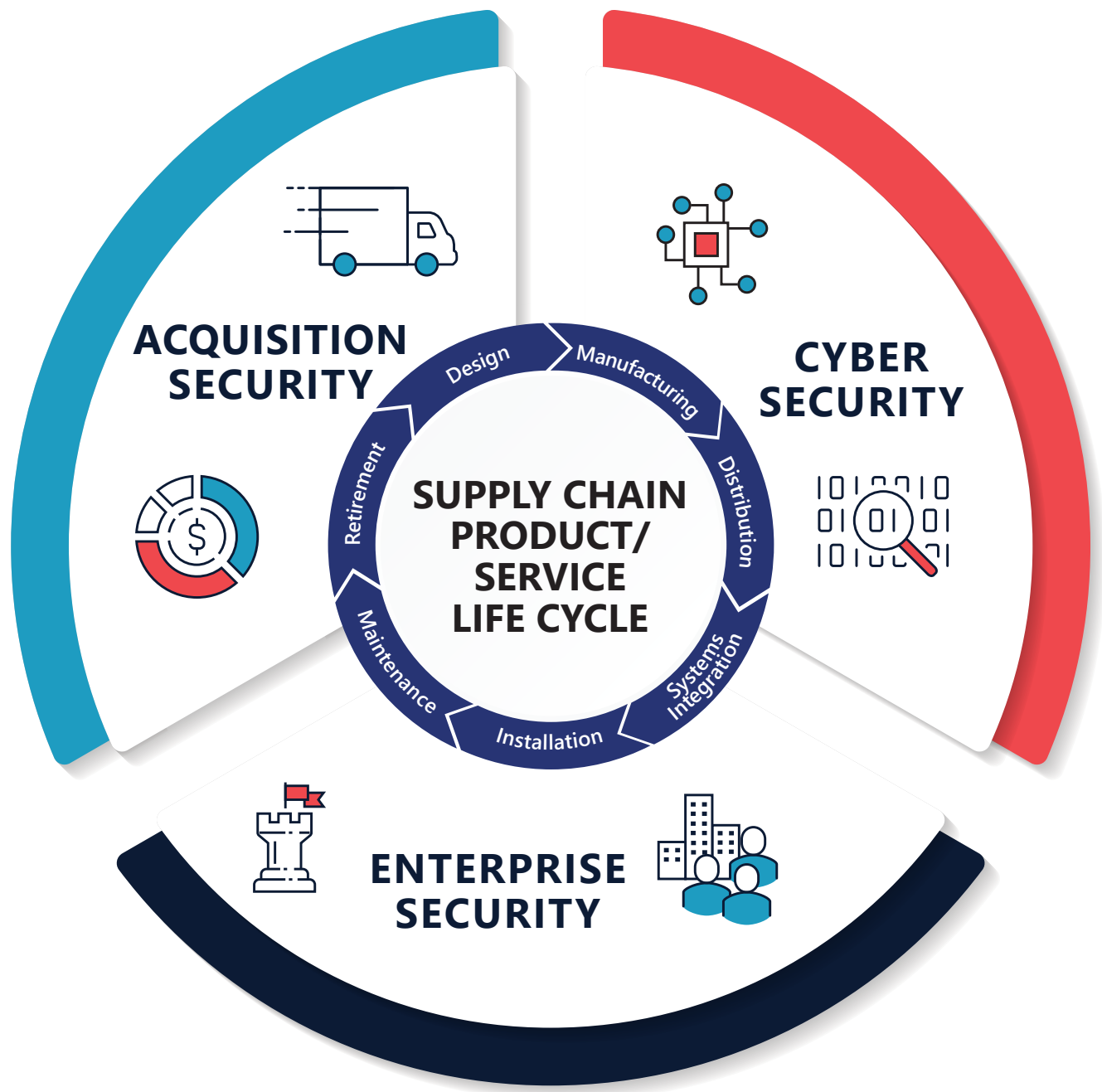
CYBER RISKS

The ICTS supply chain—or “cyber” supply chain—is the primary threat vector leveraged by threat

actors for conducting economic espionage, stealing intellectual property, and accessing sensitive U.S. data. Continued supply chain attacks have tested the security of the global cyber supply chain that supports all aspects of society. The complex network of relationships between customers, suppliers, vendors, and third-party service providers compounds the increasingly sophisticated threat against globally sourced goods and services leveraged throughout our digital infrastructure. Preventing a cyber supply chain attack can be achieved by mapping your supply chain, identifying critical path systems and information, evaluating your attack surface, and addressing all cyber vulnerabilities commonly used by threat actors.

ENTERPRISE RISKS

As the threat level from adversaries increases, public and private sector organizations holding sensitive data become more at risk. Insiders can pose significant risk to the supply chain as they can cause harm through economic espionage, sabotage, fraud, negligence, and other misuse of enterprise resources. An unwitting employee’s click on a malicious link can bring an organization to a halt. Further, a supplier’s physical security posture may leave an organization’s employees and assets vulnerable. To reduce these risks, organizations should implement employee training designed to help employees identify potential risks to its supply chain from insiders and suppliers. They should also develop strategies to mitigate such risks and integrate these security principles into the existing organizational risk management program.



SUPPLY CHAIN SECURITY

Security-driven principles can address these risks to the supply chains that organizations rely upon every day. Acquisition, cyber, and enterprise security best practices can be implemented to bolster SCRM programs beyond traditional cost, schedule, and performance. Adversaries use the complexity and opacity of supply chains to obfuscate their efforts to obtain sensitive research, intellectual property (IP) and personal data. Further, supply chain access to critical digital networks provides adversaries with the opportunity to insert malware, hide foreign ownership, control, and/or influence (FOCI) ties, and counterfeit or manipulate key components and services. By incorporating security-driven principles, organizations can bolster their SCRM programs to reduce the scale, scope, and severity of these hostile supply chain threats.

Acquisition security will help organizations navigate the globalization of supply chains, which is characterized by a complex web of contracts and subcontracts for goods and services around the world. Cyber security is an absolutely critical component to supply chain security. Adversaries can leverage the digital infrastructure to access global supply chains at multiple points, establishing advanced, persistent, and multifaceted subversion. At the enterprise level, organizations must incorporate security principles to address insider threats, third-party risks, legal constraints, geopolitical tensions, and supplier diversification. Individually and in total, these supply chain security principles will reinforce an organization's supply chain resilience.

FIXABLE OR FATAL?



CRITICALITY

Assessing risks is time consuming for any organization. A criticality assessment is a key driver for determining the need for a full SCRM assessment. This assessment includes an end-to-end performance review of the critical functions of the item or service based on a determination of the potential harm caused by the probable loss, damage, or compromise of a product, material, or service. If the item fails to perform as designed and the results of that failure are fatal to the mission, the acquisition is deemed critical and thus should be prioritized for a full SCRM assessment. If the failure can be fixed, then the

acquisition may not need a full SCRM assessment. Conducting criticality assessments provides a foundational baseline for organizations to prioritize SCRM assessments for supply chain resiliency.

CONSEQUENCE

Understanding threats and vulnerabilities allow an organization to conduct a consequence or "likelihood" analysis. This analysis can reveal the probability of an exploitation of a vulnerability by an adversary causing a compromise of a supply chain. The objective is to assess the net effect

of the vulnerability to determine the likelihood of a successful attack. The consequence analysis allows an organization to determine its recovery and resiliency plans for continuing to operate—answering the question of “Is the supply chain compromise fixable or fatal?”

IMPACT

Organizations can leverage the consequence analysis to assess the impact to the organization. The impact analysis evaluates the effect of a loss of confidentiality, integrity, or availability due to the successful exploitation of a vulnerability by an adversary. Impact analyses should include an organizational stakeholder review of enterprise-level requirements, loss of information data, costs, legal liabilities and penalties, reputational concerns, and loss of productivity. This review may also include mitigation strategies that align with the strategic goals of the organization.

SUPPLY CHAIN RISK TOLERANCE

NCSC is responsible for implementing the Intelligence Community Standards (ICS) for Intelligence Community Directive (ICD) 731, Supply Chain Risk Management. ICD 731 calls for a criticality assessment of any mission critical

products, materials, or services to be acquired.

Full supply chain risk assessments will assist organizations in determining their supply chain risk tolerance. Organizations need to know what’s the higher risk: exposure to the supply chain threat or not receiving the goods and services. Such determinations cannot be made in a vacuum. Organizational stakeholders must understand their role in addressing supply chain risks at the enterprise level.

Supply chain risk management can be incorporated into existing risk management processes, such as those described in *Managing Information Security Risk* (NIST SP 800-39), the *NIST Framework for Improving Critical Infrastructure* (the Cybersecurity Framework) and *Integrating Cybersecurity and Enterprise Risk Management* (NISTIR 8286).

Following the steps and activities in these frameworks involves framing the risk, assessing identified risks, and deciding a range of appropriate responses to reduce the risks to an acceptable level. These frameworks incorporate risk monitoring activities to ensure residual (accepted) risks remain within the organization’s risk tolerance level.

KEY ORGANIZATIONAL COMPONENTS

SCRM organizational models have evolved in public and private sectors. In the past, supply chain was often managed by a subordinate office within the acquisition or contracts office without input from other organizational stakeholders. Further, supply chain offices were usually focused on compliance-based activities driven by cost, schedule, and performance metrics.

Today, organizations that have evolved from a compliance-based model to a risk-based model have discovered risks to their organizations that would most likely not have been identified under a compliance-based regime. Responding to today's supply chain threats requires a risk-based model approach in order to maintain resiliency.

A multi-disciplinary approach is needed to achieve supply chain security and includes input from several key organizational components, including:

- Acquisition/Contracts Security
- Physical Security
- Counterintelligence
- Legal and Policy
- Information Technology
- Research and Development
- Insider Threat
- Human Resources
- Finance
- Logistics



A risk-based approach incorporates input from multiple organizational components to address supply chain threats from multiple vectors. This elevates supply chain security to ensure that an organization's leadership incorporates supply chain risks into the organization's overall risk assessment.

By incorporating these disciplines into SCRM risk assessments, stakeholders will enable the organization to make better enterprise decisions to reduce risk and build resilience.

ORGANIZATIONAL ROLES AND RESPONSIBILITIES



► ACQUISITION/CONTRACTS

Acquisition in SCRM is essential in identifying viable sources of supply, soliciting bids, and evaluating offers. In addition to cost, schedule, and performance of potential vendors or suppliers, Acquisition should also assess security and include specific cybersecurity risk requirements in the acquisition process.



► LEGAL & POLICY

Legal and policy input into SCRM programs will help organizations identify legal risks, including liabilities, contract breaches, and IP protections. Legal review of third-party contracts is also key to minimizing organizational risk.



► INSIDER THREAT

The designated senior Insider Threat program official and program staff are responsible for assessing supply chain risk from insiders, both witting and unwitting. Educating personnel on how to spot an insider threat is key to SCRM mitigation strategies.



► PHYSICAL SECURITY

Ongoing coordination with Security organizations is imperative, and SCRM programs should incorporate physical security, information security, privacy, and cybersecurity actions.



► INFORMATION TECHNOLOGY

IT offices serve a critical role in SCRM programs by implementing, maintaining, and safeguarding the networks that are foundational to organizational operations.



► RESEARCH & DEVELOPMENT

A key facet in the acquisition life-cycle, R&D organizations must protect their designs, IP, and testing environments from external threats.



► LOGISTICS

Logistics professionals are organizational enablers providing end-to-end solutions for delivering goods and services for the organization.



► COUNTERINTELLIGENCE

Counterintelligence (CI) program personnel should assess risks from adversarial threats, evaluate potential CI risk mitigation alternatives, assess Foreign Intelligence Entity (FIE) threats to the supply chain, and share threat information with other organizational elements.



► HUMAN RESOURCES

HR offices ensure SCRM training and development is implemented throughout the organization. HR policies can also ensure individuals are trained in appropriate SCRM processes and procedures.



► FINANCE

Cyber threats can cause costly breaches. Finance personnel support the SCRM program by understanding the total cost of ownership for an organization's IT networks, including mitigations, liabilities, time offline, and added personnel.

RISK GOVERNANCE AND ACCOUNTABILITY

Given the importance of incorporating SCRM into an enterprise risk management program, supply chain security needs executive-level attention and a governance process for assessing, responding to, and monitoring the complex risks in this environment. A senior executive officer should be responsible for executing—with the support of a carefully selected team—a dedicated SCRM program. The SCRM program must include the appropriate stakeholders, who may be responsible, accountable, consulted, or informed depending upon their respective role in the SCRM activity.

Within such a governance structure, accountability should be a high priority. While a designated

risk executive is responsible for the program's execution, different individuals at different levels within the organization should be accountable for specific activities such as assessing supply chain risk, selecting mitigation controls, and assessing your SCRM program capability's maturity. In addition, when the designated risk executive accepts the residual supply chain risk (the risk to your organization that remains after controls are implemented), that risk acceptance should be formalized as a key step in the SCRM process. Formalizing residual risk acceptance is a best practice that will help ensure that risk information is thoroughly analyzed, understood, and communicated among your organization's stakeholders.

Examples of SCRM assignments and activities might include:



The chief information officer, or equivalent, is **accountable** for certain risk framing and risk monitoring activities, and is **consulted** on supply chain risk response actions.



The chief risk officer, or equivalent, is **consulted** on risk framing and risk response, and is **informed** of residual risk sign-off.



The chief executive officer, or equivalent, is **consulted** on high-level risk framing, and is **informed** of all other SCRM activities.



Various actors, **responsible** or **consulted** on supply chain security accountability, which is a formalized, overarching practice within your SCRM program.



THE SCRM PROGRAM AND BEST PRACTICES FOR YOUR ORGANIZATION

If an organization already has a senior executive risk official or decision-making board, processes and workflows may need to be adjusted to incorporate the unique risks from supply chain threats. This adjustment begins with assigning a SCRM program manager who has access to senior executives and establishing a SCRM team comprising the full range of organizational stakeholders. The next section outlines the

basic steps of planning and implementing SCRM policies and practices aimed at protecting organizations' sensitive information and assets. The information and references are only a guide for SCRM program development, which must be tailored to meet an organization's unique business or mission needs to properly mitigate supply chain risks.

MANAGE SUPPLY CHAIN RISK

A FOUR-STEP PROCESS

SCRM includes assessing and responding to risk introduced through the organization's supply chain processes, including potential access by adversaries to products and services prior to acquisition as well as risk that emerges over the life cycle of a product or service. The comprehensive process outlined by the National Institute of Standards and Technology (NIST) for managing cyber supply chain risk comprises the following four steps:

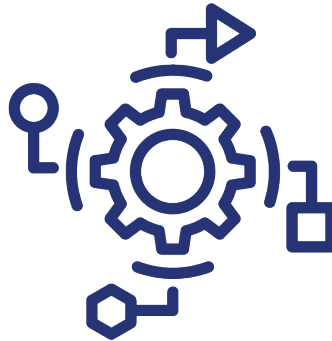
- 1. FRAME RISK.** Establish the context for risk-based decisions and define the scope and structure of the enterprise supply chain, the overall risk management strategy, and individual information systems.
- 2. ASSESS RISK.** Conduct a risk assessment based on assumptions, established methodologies, and collected data.
- 3. RESPOND TO RISK.** Communicate the assessment results, proposed mitigation options and the corresponding acceptable level of risk for each proposed option to decision makers.
- 4. MONITOR RISK.** Verify compliance, determine the ongoing effectiveness of risk response measures, and identify risk-impacting change to enterprise information systems.

The figure below describes activities that may be performed at each step of the SCRM process by SCRM personnel (described in greater detail in NIST Special Publication 800-161 r1, Appendix

G, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations). The steps summarized in this process are iterative but not necessarily performed in sequence.

	FRAME	ASSESS	RESPOND	MONITOR
 ORGANIZATION	• Develop SCRM Policy • Conduct baseline criticality determination	• Integrate SCRM into enterprise management	• Make enterprise risk decisions, to avoid, mitigate, share, or transfer risk • Select and implement appropriate enterprise • SCRM controls • Document controls in enterprise SCRM plan	• Integrate SCRM into department/agency programming, planning, budgeting, execution processes • Monitor and evaluate enterprise-level change in risk information • Monitor effectiveness of enterprise-level risk response
 MISSION OUTCOMES	• Define SCRM mission or business requirements • Determine SCRM risk assessment methodology	• Conduct risk assessment—including criticality analysis—on all mission or business functions	• Make mission- or business-level decisions to avoid, mitigate, share, or transfer risk • Select and implement appropriate mission- or business-level SCRM controls	• Integrate SCRM into department/agency programming, planning, budgeting, execution processes • Monitor and evaluate enterprise-level change in risk information
 SYSTEMS	• Define system-level SCRM requirements	• Conduct risk assessments—including criticality analysis—for all individual systems	• Make mission- or business-level decisions to avoid, mitigate, share, or transfer risk • Select and implement appropriate system-level SCRM controls	• Monitor and evaluate system-level change in risk information • Monitor effectiveness of system-level risk response

FRAME



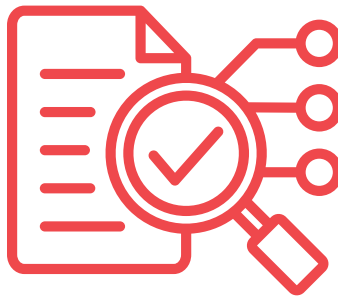
The Frame step defines the scope and structure of your organization's supply chain infrastructure, your organization's risk management strategy, and the analytic requirements for specific acquisitions and systems. Risk framing is the set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization's

approach for managing risk. NIST 800-161, r1., Appendix G. Relevant outputs of this process might include an understanding of your organization's known threats and vulnerabilities, the laws and regulations that may apply to your SCRM practice, or the functional or security requirements for your organization.

▶ After framing your supply chain risk, your program team should have some understanding of how your organizational **SCRM policy** will take shape. You should also have examined **baseline criticality**, including your approach to prioritizing the functions critical to your mission or business. Additionally, the framing step will inform notional **guidance for your organization's supply chain risk assessment (including a methodology)**, **risk response**, and **risk monitoring** practices.

Additionally, your SCRM team members should have a general understanding of the **SCRM requirements** that will be implemented throughout the organization in support of risk mitigation activities.

ASSESS



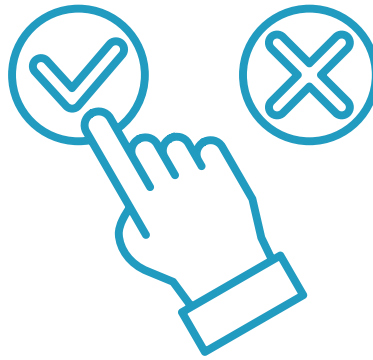
The Assess step of the SCRM process requires the organization to combine and analyze a number of inputs—including criticality, threat, and vulnerability analysis results; stakeholder insights; and policy issues, constraints, and requirements—in order to determine the likelihood and impact of a supply chain compromise. Since the supply chain risk assessment should be integrated into your organization’s enterprise risk assessment

processes, SCRM risk assessment results should be communicated, as appropriate, to inform actions at every organizational tier. NIST publications—including NIST SP 800-161r1 and NIST SP 800-30—provide detailed guidance and frameworks for private or public sector organizations seeking to implement sound risk assessment practices.

► Once your SCRM team assesses components of the organization’s risk, you should have a **confirmed or updated criticality analysis** that prioritizes your mission or business functions and systems. Your threat and vulnerability analyses should help your team **understand the relationships between each critical aspect of your supply chain and the threats and vulnerabilities associated with it**, as well as the **likelihood and impact of any potential supply chain compromise**.

This common understanding of mission- and system-specific risks should be supported by **documented supply chain risk assessments** for mission or business functions and for individual systems. Finally, relevant supply chain risk assessments results should be fully integrated into the organization’s overall risk management process.

RESPOND



In the Respond step, SCRM program officials conducting the risk assessment communicate the assessment results, proposed alternatives for responding to the risk, and corresponding acceptable risk levels for the proposed alternatives to inform risk-based decisions. Decision makers consider the risk factors associated with the proposed responses and

select the appropriate risk response based on that information. Choosing to not respond to the risk and instead monitoring the adversary's activities can be an appropriate response if risk remains within an acceptable range. Like other steps in the SCRM process, supply chain risk response should be integrated into your organization's overall risk response.

▶ Executing these steps should result in a set of **SCRM controls your team has selected and tailored** to address identified risks to your supply chain. These controls represent the core of your organization's supply chain risk mitigation activities, and your team members should **identify and understand the consequences of accepting or not accepting any proposed mitigations** in order to fully understand the overall SCRM strategy.

The **development and implementation of your organization's SCRM plan** will document the evaluation, selection, and execution of these controls and provide context for evaluating the effectiveness of your mitigation decisions and activities, as well as the maturity of your SCRM capability.

MONITOR



In the Monitor step, the SCRM program is regularly evaluated to maintain or adjust the acceptable level of risk. Changes to your organization—or its supply chain—are regularly monitored to determine their impact on the supply chain infrastructure which should be

re-evaluated during the assessment step. If any changes in the supply chain infrastructure occur as a result of monitoring, the relevant information should be immediately shared with supply chain stakeholders.



Your organization should **integrate the supply chain outputs of the risk monitoring into the SCRM plan**. This plan will provide inputs into subsequent iterations of the Frame, Assess, and Respond steps as required.

As a best practice, you should **develop and implement a capability maturity model (CMM)** to track your SCRM program's progress on implementation and technical objectives.

WHAT'S NEXT?

The information contained in this document should help you tailor your SCRM program to the particular characteristics of your organization. The following tables summarize recommended actions that make up the SCRM process steps, provide a checklist of the basic outputs that the process steps should produce, and give an example of a breakdown of responsibilities for your SCRM team.

The basic SCRM process steps are summarized below. The reference materials cited below can also provide additional assistance in tailoring SCRM programs to the unique characteristics of each organization.

FRAME	ASSESS	RESPOND	MONITOR
-------	--------	---------	---------

After framing SCRM risks, program teams should have some understanding of how organizational SCRM policies will take shape. Baseline criticality should also be examined, including approaches to prioritizing the functions critical to missions or businesses. Additionally, the framing step will inform notional guidance for an organization's supply chain risk assessment (including a methodology), risk response, and risk monitoring practices.

FRAME	ASSESS	RESPOND	MONITOR
-------	--------	---------	---------

Once SCRM teams assess components of organizational risk, there should be a confirmed or updated criticality analysis that prioritizes mission or business functions and systems. Threat and vulnerability analyses should help program teams understand the relationships between each critical aspect of the supply chain and the threats and vulnerabilities associated with it, as well as the likelihood and impact of any potential supply chain compromise.

FRAME	ASSESS	RESPOND	MONITOR
-------	--------	---------	---------

Executing these steps should result in a set of SCRM controls selected and tailored to address identified risks to organizational supply chains. These controls represent the core of an organization's supply chain risk mitigation activities, and team members should understand the consequences of accepting or not accepting any proposed mitigations as part of the overall SCRM strategy.

The development and implementation of an organizational SCRM plan will document the evaluation, selection, and execution of these controls and provide context for evaluating the effectiveness of mitigation decisions and activities, as well as the maturity of SCRM capabilities.

FRAME	ASSESS	RESPOND	MONITOR
-------	--------	---------	---------

Organizations should integrate the supply chain outputs of the risk monitoring into the SCRM plan, which will provide inputs into subsequent iterations of the Frame, Assess, and Respond steps.

As a best practice, capability maturity models (CMMs) should be developed and implemented to track a program's progress on implementation and meeting technical objectives.

SCRM IMPLEMENTATION: ACTIONS AND OUTPUTS

This table identifies prescribed actions under each of the SCRM program steps that will lead to expected outputs from SCRM programs. It can serve as an initial checklist for early iterations of a SCRM process.

				
	FRAME	ASSESS	RESPOND	MONITOR
ESSENTIAL ACTIONS	1. IDENTIFY RISK ASSUMPTIONS that affect how risk is assessed, responded to, and monitored within the organization. 2. IDENTIFY THE CONSTRAINTS on the conduct of the risk assessment, risk response, and risk monitoring activities. 3. DETERMINE THE RISK TOLERANCE for your organization. 4. DETERMINE THE PRIORITIES and trade-offs to be considered within the risk management process.	1. PERFORM OR UPDATE A CRITICALITY ANALYSIS of functions, systems, and components to narrow the scope for SCRM activities to those most important to protecting sensitive information and assets. 2. IDENTIFY THREATS AND VULNERABILITIES associated with your organization's acquisitions and systems and the environments in which they operate. 3. DETERMINE THE RISK to sensitive information and assets if the identified threats exploit the identified vulnerabilities.	1. IDENTIFY ALTERNATIVE COURSES OF ACTION to respond to risk determined during the risk assessment. 2. EVALUATE ALTERNATIVES FOR RESPONDING to the identified risk. 3. DETERMINE THE APPROPRIATE COURSE OF ACTION for responding to the risk. 4. IMPLEMENT THE COURSE OF ACTION selected to respond to risk.	1. DEVELOP A RISK MONITORING STRATEGY for the organization that includes the purpose, type, and frequency of monitoring activities. 2. MONITOR SYSTEMS AND ENVIRONMENTS OF OPERATION on an ongoing basis to verify compliance with controls, determine the effectiveness of risk response measures, and identify appropriate changes.
	□ SCRM policy □ Baseline criticality □ Guidance for SCRM risk assessment, risk response, and risk monitoring practices □ SCRM requirements	□ Confirmed or updated criticality analysis □ Threat analyses for individual systems □ Vulnerability analyses for individual systems □ Likelihood and impact analyses for individual systems □ SCRM risk assessments for business functions and individual systems □ Integration of SCRM risk assessments into enterprise risk management process	□ Selected and tailored SCRM controls □ Understanding of residual risk and consequences of accepting or not accepting proposed mitigations □ Development and implementation of organizational SCRM plan	□ Integration of SCRM monitoring outputs into the SCRM plan □ Development and implementation of CMM
EXPECTED OUTPUTS				

EVALUATING YOUR ORGANIZATION'S SCRM PROGRAM

RESOURCE COMMITMENT

SCRM programs require dedicated resources to ensure that such risks are identified, prioritized, and mitigated. Leveraging the information in this guide will assist in tailoring a SCRM program that incorporates the appropriate policies and practices to address the organization's supply chain risks. Resourcing a SCRM program can seem costly; however, such costs are minimal when compared to the costs of suffering a supply chain compromise, exploitation, or shock.

COMPLIANCE MAY LEAD TO COMPLACENCY

Most organizations are unaware of their risk exposure, but understanding these security risks, especially cyber-related risks, is essential to preventing the exploitation of your organization's vulnerabilities through the global supply chain. Due diligence must be exercised to understand the provenance of the technologies and the suppliers. Organizations cannot become complacent with supply chain security.

TRAIN YOUR ORGANIZATION'S STAKEHOLDERS

As the degree of threats from adversaries increases, the risks to private and public sector organizations are deepening. SCRM stakeholders must lead the organization in identifying potential risks to sensitive information and develop strategies to reduce those risks. Trained SCRM stakeholders should be included in all risk discussions, and their collective input should be integrated into the existing organizational risk management program.

Supply chain disruptions will continue to plague public and private sectors, leading to excessive shortages, delays, and added costs for basic commodities and services. So many aspects of our lives—government, businesses, schools, healthcare, and social services—are moving to digital platforms, and adversaries are preying on this digital infrastructure. With the commitment of senior management resources and trained stakeholders, SCRM will help any organization navigate evolving supply chain risks.



REFERENCES AND RESOURCES

For additional information on managing supply chain risks, cyber risks, acquisition risks, and enterprise risks, please see the guidance below:

- NIST SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
- NIST SP 800-39: Managing Information Security Risk: Organization, Mission, and Information System View
- NIST CSF 2.0: Cybersecurity Supply Chain Risk Management (C-SCRM)
- NISTIR 8179: Criticality Analysis Process Model
- NIST SP 800-61R2: Computer Security Incident Handling Guide
- NIST Special Publication 800-181, revision 1: Workforce Framework for Cybersecurity (NICE Framework)
- NISTIR 8276: Key Practices in C-SCRM: Observations from Industry
- Center for Development of Security Excellence: Insider Threat Toolkit
- GSA Cybersecurity Supply Chain Risk Management (C-SCRM) Acquisition Guide



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

For more information on supply chain security, please visit [ncsc.gov](https://www.ncsc.gov)