SCRM ESSENTIALS

Information and Communications Technology Supply Chain Risk Management (SCRM) in a Connected World

THE LEADER'S GUIDE

Protecting your organization's information in a digitally connected world demands an understanding of third-party vendor supplier security. Consider which organizations are in your supply chain and whether you trust the hardware, software, and services you receive. As with other risks, supply chain risks can threaten:

- **YOUR ABILITY TO OPERATE/ACCESS INFO**
- **YOUR REPUTATION/CUSTOMER TRUST**
- **YOUR BOTTOM LINE**
- **YOUR ORGANIZATION'S RESILIENCE**

Managing supply chain risks requires building an effective supply chain management practice and understanding extended supply chains that consist of suppliers, vendors, and service providers.

Essential Steps to Building an *Effective Supply Chain Risk Management Practice:*

Step 1 — Identify *- The People*

Determine who from your organization needs to be involved

Build a team of representatives from various roles and functions of the company (e.g., cybersecurity, information technology, physical security, procurement/acquisition, legal, logistics, marketing, and product development). Ensure personnel at all levels are well-trained in the security procedures of their role or function.

This team will bring together diverse perspectives of subject matter experts from across your organization.

Step 2 — Manage *- The Security and Compliance*

Develop your supply chain security policies and procedures

Document the set of policies and procedures that address security, integrity, resilience and quality. Ensure they are based on industry standards and best practices on how to conduct supply chain risk management, such as those from the National Institute of Standards and Technology (NIST).[1]

Promote a leadership-encouraged culture of supply chain readiness.

Step 3 — Assess *- The Components*

Understand the hardware, software, and services that you procure

Build a list of the information and communications technology (ICT) components (e.g., hardware, software, services) that your organization procures to enable your business. Know which internal systems are relied upon for critical information or functions, and which systems have remote access capability that must be protected to prevent unauthorized access.

Step 4 — Know *- The Supply Chain and Suppliers*

Map your supply chain to better understand what components you procure

Identify your suppliers and, when possible, the suppliers' sources. In today's world of increased outsourcing, it is important to understand your upstream suppliers as part of the larger supply chain ecosystem.

Consider suppliers of critical components as well as those that provide assets, systems, and data that enable your business.

Step 5 — Verify *- The Assurance of Third Parties*

Determine how your organization will assess the security culture of suppliers

Verify that your suppliers maintain an adequate security culture and supply chain risk management program to appropriately address the risks that concern your organization. Establish the protocols your organization will use to assess the supply chain practices of your suppliers.

Consider the types of frameworks, models, qualification criteria, contractual clauses and monitoring you will use to assure trusted supply chain practices.

Step 6 — Evaluate *- The Review*

Establish timeframes and systems for checking supply chain practices against guidelines

Determine the frequency with which you will review your SCRM program, incorporate feedback, and make changes to your risk management program. This may also include auditing suppliers against practices and protocols established by your organization.

Your supply chain risk management program will continuously move through these steps.

[1] To learn more about SCRM-related key practices (e.g., NIST SP800-161, NISTIR 8276), news, and latest projects, visit the NIST's webpage at **https://csrc.nist.gov/Topics/Security-and-Privacy/supply-chain**.

www.CISA.gov/NRMC-SCRM

flip page ▶

STARTING UP

Understand First ▸

- Your Suppliers
- Your Vendors
- Your Service Providers
- Your Components

SCRM ESSENTIALS

THE SUPPLY CHAIN GUIDE

Essential Actions for Building a ***Culture of Supply Chain Risk Management***

Essential Actions Legend

- ▲ *Actions for leaders.*
- ○ *Actions for staff.*

Identify

Determine who from your organization needs to be involved.

Organizations can:

- ▲ Integrate representatives from multiple functions within your organization into one larger supply chain program.
- ▲ Include subject matter experts in cybersecurity, information technology, product development and security, legal, logistics, physical security, acquisition, marketing, and leadership.
- ▲ Bridge offices to create information sharing, metrics, and program objectives that will ultimately reduce supply chain risks.
- ▲ Recognize that for larger organizations, this will result in a larger team; for smaller organizations, this may be a few key individuals.
- ○ Include representatives from all levels of the organization, to include operators.

Manage

Develop your supply chain security policies and procedures.

Organizations can:

- ▲ Direct the establishment of an enterprise-wide supply chain risk management program.
- ▲ Establish standard operating procedures on how to conduct supply chain risk management and maintain compliance, to include training.
- ▲ Lead policy development.
- ▲ Establish clear governance of activities.
- ○ Identify and obtain industry standards and best practices which can define your organization's policies.
- ▲ Promote supply chain risk management as a business priority.

Assess

Understand the hardware, software, and services that you procure.

Organizations can:

- ▲ Understand the critical information in your organization and where it resides.
- ○ Determine the different parts of your information and communications technology supply chain.
- ○ Identify, assess, and prioritize critical assets, systems, processes, and suppliers.
- ○ Determine the hardware, software, and managed services most pertinent to your organization.
- ○ Track the critical components that your organization procures.

Know

Map your supply chain to better understand what components you procure.

Organizations can:

- ○ Answer the question: From which companies do you procure your assets, hardware, software, and services?
- ○ Answer the question: Do your key suppliers have assurance programs in place? Consider asking for information about their supply chain risk management practices.
- ○ Consider whether you can build, leverage, or utilize an approved supplier list.
- ○ Limit suppliers' access to only the data they need to conduct business.

Verify

Determine how your organization will assess the security culture of suppliers.

Organizations can:

- ○ Set standards for your vendors in terms of their systems, processes, and extended supplier security requirements.
- ○ Establish security requirements (e.g., on-site security).
- ○ Set service-level agreements requiring suppliers to adhere to security policies.
- ○ Identify methods for assessing assurance and how they will be measured (e.g., self-attestation, auditing).
- ○ Determine how information will be shared within your organization.

Evaluate

Establish systems for checking supply chain practices against guidelines.

Organizations can:

- ▲ Establish security as a primary metric (just like cost, schedule, and performance) for assessing a vendor's ability to meet contract requirements.
- ▲ Identify and implement mitigation measures.
- ○ Implement the program and monitor suppliers' and your organization's adherence to SCRM requirements.
- ○ Determine the schedule at which systems will be monitored against guidelines.

To learn more about CISA Supply Chain Risk Management programs, visit www.CISA.gov/NRMC-SCRM.