TEVORA™ | White Paper

NAVIGATING SP 800-161 REV. 1:

Best Practices for Cybersecurity Supply Chain Risk Management in Systems and Organizations

Author: Thomas Feeley (Federal Team)
Assisted: Riley Webber (Third Party Risk Management)

Introduction

In 2015, the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-161, titled "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," was introduced as a response to the Federal Information Security Modernization Act of 2014 (FISMA 2014). However, with the advent of the SECURE Technology Act, FASC Finale Rule, and Executive Order (EO) 14028, also known as "Improving the Nation's Cybersecurity," a revised version was published in May 2022. This revision broadens the scope beyond federal agencies, emphasizing the significance of managing cybersecurity risks within supply chains.

Tevora as, a certified third-party assessment organization (3PAO), is dedicated to delivering timely updates and valuable insights regarding the most recent cybersecurity guidelines and best practices. In this white paper, we will delve into the intricate aspects of modern supply chains, emphasizing the significance of visibility, transparency, and the need for internal and external collaboration. Furthermore, we will explore integrating of these practices with broader enterprise policies and processes, the importance of business continuity and resilience, and highlight the crucial role of Cybersecurity Supply Chain Risk Management (C-SCRM). These topics will be discussed within the updated document "SP 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations."

Overview of SP 800-161 Rev. 1

NIST SP 800-161 Rev. 1 offers a comprehensive guide to the benefits of supply chain risk management (SCRM) practices, extending relevance beyond federal information systems to all organizations. This document underscores the advantages of managing risks effectively within the global supply chain for information communications technology (ICT) products and services, emphasizing the crucial role of stakeholder collaboration.

A pivotal aspect of this collaboration involves understanding the roles and responsibilities of various stakeholders across different levels of an organization. SP 800-161 Rev. 1 provides a detailed framework outlining how stakeholders, from executive leadership to operational systems management, can contribute to effective SCRM.

As we delve into the intricacies of modern supply chains and explore how SP 800-161 Rev. 1 bolsters an organization's SCRM strategies, it's important to keep these stakeholder roles in mind. This understanding will enable us to identify key controls and devise effective risk mitigation strategies.

To enhance our understanding of these roles and responsibilities, let's examine the stakeholder activities as outlined in SP 800-161 Rev. 1 in the following table.

LEVEL	STAKEHOLDER GROUP	KEY ACTIVITIES
1	Enterprise Executive Leadership: CEO, CIO, COO, CFO, CISO, CTO, CAO, CPO, CRO, etc.	• Define enterprise CSCRM strategy • Form governance structures and operating models • Frame risk for the enterprise and set risk appetite • Define high-level implementation plan, policy, goals, and objectives • Make enterprise-level CSCRM decisions • Form a C-SCRM PMO
2	Mission and Business Process: Program management, project managers, R&D, engineering, acquisition and supplier relationship management, etc.	• Develop mission and business process-specific strategy • Develop policies, procedures, guidance, and constraints • Reduce vulnerabilities at the onset of new IT projects and/or related acquisitions • Review and assess system, human, or organizational flaws that expose environments to cyber threats and attacks • Develop C-SCRM implementation plan(s) • Tailor the enterprise risk framework to the mission and business process • Manage risk within mission and business processes • Form and/or collaborate with a C-SCRM PMO • Report on C-SCRM to Level 1 and act on reporting from Level 3
3	Operational Systems Management: Architects, developers, system owners, QA/QC, testing, contracting personnel, C-SCRM PMO staff, control engineer and/or control system operator, etc.	• Develop C-SCRM plans • Implement C-SCRM policies and requirements • Adhere to constraints provided by Level 1 and Level 2 • Tailor C-SCRM to the context of the individual system, and apply it throughout the SDLC • Report on C-SCRM to Level 2

Managing the Complexity of Modern Supply Chains

The complexities of modern supply chains arise from a confluence of factors. Globalization has forced supply chains to become more interconnected, expanding the attack surface across countries and regions. This interconnectedness is not merely a characteristic of modern supply chains but a necessity driven by efficiencies in cost, speed, and expanded market reach.

Each stage in a supply chain, from raw material sourcing to final product delivery, presents an opportunity for vulnerabilities to arise. The high degree of interdependence between components and stakeholders within the supply chain amplifies these vulnerabilities; disruptions in one area can have far-reaching impacts. The importance of addressing third-party vulnerabilities, as emphasized in NIST SP 800-161 Rev. 1, comes into play.

An organization's cybersecurity is often only as strong as its weakest third-party supplier. For this reason, NIST SP 800-161 Rev. 1 emphasizes the importance of addressing third-party vulnerabilities in supply chain security. Organizations are advised to establish a consistent risk management process to identify and mitigate potential risks from third-party suppliers and service providers. The first essential element of this management process is visibility and transparency.

Visibility and Transparency

Similar to managing system vulnerabilities, attaining visibility and transparency are the first critical steps toward managing supply chain risk. Enhancing these aspects involves:

- Developing a detailed inventory of all components, services, and suppliers within your supply chain.
- Establishing clear communication channels with all supply chain partners.
- Implementing real-time monitoring and tracking systems.
- Evaluating supplier relationships regularly.
- Collaborating with industry partners to share best practices and threat intelligence related to supply chain risks.

These steps help manage third-party vulnerabilities and contribute to the overall resilience and continuity of business operations. The second pivotal component of the management process: the vital role of collaboration in effectively mitigating supply chain risks.

Collaboration with Internal and External Stakeholders

The success of SCRM programs relies heavily on clear communication between all stakeholders. This includes supply chain partners and internal personnel from various disciplines and departments (e.g., information security, procurement, legal, HR, privacy). Recognizing the importance of such collaboration is the first step toward a functional SCRM program.

Expanding on this notion, NIST SP 800-161 recommends formally integrating C-SCRM into the broader enterprise-wide risk management process. This should be a continuous and iterative program, encompassing the framing, assessment, response, and monitoring of risk within the enterprise's systems and its extended third-party ecosystem. Such a change requires an enterprise-wide cultural shift towards a heightened awareness and preparedness for the potential implications of cybersecurity risks throughout the supply chain. Supporting this integration leads us to the third element in our management process, which involves enterprise policies and procedures.

Integration with Wider Enterprise Policies and Processes

NIST SP 800-161 describes taking a multilevel, multidisciplinary approach when implementing risk management processes to ensure optimal efficacy. The approach often begins with developing a policy and program (Level 1). These foundational elements are then used to design processes based on the organization's resources and strategic objectives, such as utilizing of a Third-Party Risk Management (TPRM) solution with supporting procedure and workflow documentation (Level 2). Finally, the program is operated, and processes are executed accordingly, with any identified risks undergoing the appropriate treatment (Level 3). With the levels defined, the supporting departments' roles must be well-defined to avoid process failures. In the same way, organizations cannot practice good cyber hygiene without the involvement of all personnel; TPRM, and therefore SCRM, cannot function without the support of all stakeholders. All relevant policies and procedures should explicitly describe each department's roles and responsibilities within the TPRM process and create workflows to align these responsibilities efficiently.

Evolving the Program

With a well-structured framework and robust processes in place, the core components of the C-SCRM program should be evaluated on an ongoing basis to identify additional areas for improvement. This evaluation can be guided by quantitative performance metrics toward C-SCRM objectives, such as the number of third parties assessed, risks successfully mitigated, and overall risk exposure from critical suppliers.

These types of performance measurements provide a periodic glimpse into the enterprise's progress through the lens of specific operational objectives. They emphasize the importance of continual improvement to stay ahead of supply chain risk.

As we delve deeper into the process of evolving the C-SCRM program, it's crucial to understand the measurement topics across different risk management levels. NIST SP 800-161 provides a detailed framework for this, outlining how measurement topics can guide the evaluation and improvement of the C-SCRM program across different levels of an organization.

To enhance our understanding of these measurement topics and how they can be applied in the context of C-SCRM, let's examine them as outlined in SP 800-161 in the following table. This table will serve as a practical tool for organizations to track their progress and identify areas of improvement in their C-SCRM initiatives.

Table 1-2: Example Measurement Topics Across the Risk Management Levels

RISK MGMT LEVEL	EXAMPLE MEASUREMENT TOPICS
1	• Policy adoption at lower levels • Timeliness of policy adoption at lower levels • Adherence to risk appetite and tolerance statements • Differentiated levels of risk exposure across Level 2 • Compliance with regulatory mandates • Adherence to customer requirements
2	• Effectiveness of mitigation strategies • Time allocation across C-SCRM activities • Mission and business process-level risk exposure • Degree and quality of C-SCRM requirement adoption in mission and business processes • Use of a C-SCRM PMO by Level 3
3	• Design effectiveness of controls • Operating effectiveness of controls • Cost efficiency of controls

How C-SCRM Benefits Your Organization

Integrating C-SCRM becomes a fundamental element of an organization's cybersecurity architecture in a globally interconnected business environment. NIST SP 800-161 Rev. 1 provides a comprehensive framework that assists organizations in understanding, identifying, and managing the cybersecurity risks present within their supply chains, contributing to preserving data integrity, system protection, and sustaining operational continuity and resilience.

ACQUISITIONS

Products, companies, and novel technologies are continually acquired to further business goals, and C-SCRM ensures these acquisitions do not hinder success by introducing excessive risk. Specifically, C-SCRM offers organizations complete insight into what may be purchased by performing proper due diligence on services, suppliers, and products. No acquisition is free of risk; however, with a clear view of what risks are being absorbed, an organization can prepare and mitigate in advance rather than being surprised by a security incident – always better to be proactive than reactive.

BUSINESS CONTINUITY AND RESILIENCE

It was often the thought that an enterprise would feel a minimal effect from a third-party data breach, but this misconception has been disproven. There are many ways for an external organization's breach to significantly impact one's own, the most critical of which is when this third party is a direct member of your business's supply chain.

An organization must maintain a clear view of how the business operates, and when developing business continuity and disaster recovery scenarios, the supply chain must be included. C-SCRM processes, following NIST 800-161 guidance, promote considering these types of risks when a prospective supplier is being evaluated. Is there a more secure alternative? Are redundancy options available? Are the proper recovery time objectives and recovery point objectives in place? These are the questions that the modern organization will be able to answer so the benefits of an interconnected supply chain can be reaped while minimizing potential downsides.

REGULATORY COMPLIANCE

Many industries and jurisdictions have specific requirements relating to data protection while more and more have been explicitly addressing controls within TPRM and SCRM (e.g., HITRUST, NIST SP 800-53 Revision 5, HIPAA, ISO 27001, NIST CSF, FDIC Interagency Guidance). Failure to support the controls that mitigate your organization's third-party, or supply chain risk can result in damages both from the breach (e.g., fines imposed, litigation costs, revenue lost due to operational downtime) and long-term business losses from damaged customer trust, brand recognition repair efforts, and difficulty establishing relationships with other businesses. By proving your organization prioritizes security and displaying compliance with industry-respected frameworks, the potential damages are minimized through breach avoidance, and customers are more likely to procure services from your enterprise rather than the competitor without security assurances.

IMPROVED BUSINESS RELATIONSHIPS

Customers are not the only ones more willing to do business with organizations that uphold mature security practices, and business partners are much more likely to. While a robust C-SCRM program ensures your organization minimizes risk when selecting its suppliers and partners, it also streamlines work with the other business prospects that maintain strong vetting processes. That is because the organization continually maturing its own C-SCRM program will produce lower risks on questionnaires, are more likely to possess security certifications that can be accepted in place of a questionnaire, and have dedicated resources to provide sufficient evidence and complete remediation requests to improve security posture even further.

Being actively involved in these due diligence processes sets the foundation for a long-lasting, mutualistic partnership and has become the strategy of large enterprises and government entities looking to develop a more resilient supply chain network. Additionally, these types of partnerships allow engagement with peers, business partners, suppliers, and information-sharing communities (e.g., ISACs), which can provide valuable insights into emerging cybersecurity risks and best practices for risk mitigation.

About Tevora

Tevora is a specialized management consultancy focused on cybersecurity. Our objective is to help keep your organization compliant and your brand safe. As a certified FedRAMP 3PAO and StateRAMP assessor, our federal services division provides advisory, preparatory, and formal assessment services for clients seeking FedRAMP and StateRAMP authorization. Additionally, our Third-Party Risk Management (TPRM) team is highly adept at managing the complex risks associated with third-party suppliers. With their keen insights and specialized skills, they're prepared to assist you in fortifying your supply chain against potential threats.

Contact Us

Throughout this article, we've explored and discussed numerous aspects of SP 800-161 Rev. 1. If you have questions or need assistance implementing C-SCRM within your organization, please get in touch with Tevora. Our knowledgeable team of security professionals is here to help. Contact us by phone at (833) 292-1609 or email us at sales@tevora.com. We look forward to supporting your cybersecurity efforts.

Our knowledgeable team of
security professionals is here to help.

Give us a call at (833) 292-1609 or email us at sales@tevora.com.

TEVORA™

Go forward. **We've got your back.**