EMPOWERING SMBs:
A RESOURCE GUIDE FOR DEVELOPING A RESILIENT SUPPLY CHAIN RISK MANAGEMENT PLAN

INTRODUCTION

This resource guide addresses the growing need for information and communications technology (ICT) small and medium-sized businesses (SMBs) to present a supply chain risk management (SCRM) plan for private or public sector stakeholders. The objective is to ensure the availability, integrity, and confidentiality of ICT products, services, and components throughout the supply chain while minimizing disruptions and vulnerabilities.

The U.S. Small Business Administration defines a small to medium-sized business according to a set of standards based on specific industries. Generally, these size standards are based on the number of employees or the amount of annual receipts the business has.[1] For the purposes of this document, an ICT SMB is defined as an organization with less than 500 employees.[2] Recognizing that many ICT SMBs lack dedicated risk management or SCRM expertise, this guide offers a valuable starting point for ICT SMBs to develop and tailor their own ICT SCRM plan.

Although primarily focused on the IT and Communications sectors, this guide is relevant for SMBs in any industry. By using this resource and actively engaging in SCRM, SMBs can develop an actionable SCRM plan to mitigate the risk of disruption to their supply chain, enhance their supply chain resilience, and satisfy potential requests from stakeholder procurement processes.

1 U.S. Small Business Administration. "Size standards." Last Updated June 21, 2023. https://www.sba.gov/federal-contracting/contracting-guide/size-standards. Accessed on August 7, 2023.

2 U.S. Chamber of Commerce. (2023, April, 10) "The State of Small Business Now." https://www.uschamber.com/small-business/state-of-small-business-now

KEY ROLES

ICT SMBs often perform different roles in the course of conducting their business. Accordingly, your organization should take into account the following roles when developing an ICT SCRM plan.

ACQUIRER

An SMB owner/operator/executive who aims to make a purchase where ICT supply chain security is of concern.

INTEGRATOR

An SMB integrator acquires and implements ICT products or services on behalf of their clients.

SUPPLIER

An SMB owner/operator/executive who aims to win a contract where ICT supply chain security is of concern to the prospective client.

PLAN ELEMENTS

01 BEGIN WITH AN EXECUTIVE SUMMARY

GUIDANCE AND STEPS

Your ICT SCRM plan should begin with a brief executive summary. This should include a high-level overview of the purpose, goals, objectives and the key elements of your plan.

02 IDENTIFY CRITICAL SUPPLIERS

GUIDANCE AND STEPS

Identify the suppliers that have access to or provide hardware or software, including cloud services, to your business by:

I. Creating and maintaining a list of suppliers, especially those critical to your business operations, and assess their importance in terms of impact on your business.

II. Identifying and prioritizing potential risks posed by your critical suppliers.

III. Establishing a formal process to refresh risk assessments of your critical suppliers and to identify and receive notice of potential vulnerabilities, such as financial instability, cybersecurity risks, or reputation risks.

03 IDENTIFY SUPPLY CHAIN RISKS TO YOUR CRITICAL ASSETS

GUIDANCE AND STEPS

ICT equipment and services are comprised of many components (critical and non-critical) that are often provisioned by a large number of suppliers – commonly known as the “supply chain.” To understand which critical assets and/or suppliers, if disrupted or compromised, will negatively impact your business operations, you must:

I. Identify and prioritize the hardware and software used in your operations.

II. Establish a method of receiving notice for available patches and updates to your hardware and software and apply them promptly.

III. Identify the end-of-life date for hardware and software and plan for a timely transition to updated hardware and software whenever possible.

PLAN ELEMENTS

04 IMPLEMENT SUPPLIER DIVERSITY

GUIDANCE AND STEPS

Maintaining a diverse supplier base when possible will reduce your dependence on any one supplier. Conversely, relying on a single critical supplier can increase risk to your organization if critical products or services become unavailable. This can include using a third-party providing cybersecurity services. In order to accomplish this, you should:

I. Develop supplier qualification criteria that ensures all your suppliers are consistently supplying quality products and services.

II. Build strong relationships with your suppliers and maintain open communication to address any issues or concerns that may arise.

III. Identify single points of failure in your supply chain and alternate suppliers in the event one source fails to meet your contractual requirements.

05 DEVELOP A VENDOR ATTESTATION PROCESS

GUIDANCE AND STEPS

Decisions that affect the supply chain could impact all areas of your business. These include the decision to purchase or use products, systems, or services. In order to evaluate vendors prior to making a purchase and to maintain supplier quality over time, your organization should implement processes and documentation by which suppliers attest, at the outset and regularly thereafter, to specific risk management attributes. This can be achieved by:

I. Establishing service level agreements.

II. Conducting regular audits of your suppliers to ensure that they comply with your policies and procedures, as well as any regulatory requirements.

III. Monitoring your suppliers' performance regularly to ensure they meet your business requirements and adhere to your quality standards.

PLAN ELEMENTS

06 DEVELOP A CONTINGENCY PLAN

GUIDANCE AND STEPS

Develop a contingency plan that outlines how you will respond to supply chain disruptions, including identifying alternative suppliers and appropriate backup plans to ensure continuity of business. In doing so, you should:

I. Identify criteria for declaring a supply chain disruption.
II. Develop incident management procedures that will be invoked in the event of a supply chain disruption.
III. Design and document supply chain disruption remediation and recovery strategies.
IV. Document lessons learned and improvement mechanisms after declared supply chain disruptions.

07 TRAIN YOUR EMPLOYEES

GUIDANCE AND STEPS

Train your employees on ICT SCRM best practices so that they understand the importance of managing supply chain risks and their roles in the process by:

I. Reviewing any existing training programs to see where ICT SCRM could be incorporated (e.g, acquisition training, security training).
II. Developing and updating employee training materials to include ICT SCRM elements.
III. Identifying key individuals who may need to receive specific ICT SCRM training (e.g., anti-counterfeit training) versus more generalized training for the entire organization (e.g., how to purchase goods/services).

08 CONTINUOUSLY MONITOR AND IMPROVE

GUIDANCE AND STEPS

Continuously monitor and improve your SCRM program to ensure the content remains effective and relevant to your business operations. In order to accomplish, you should:

I. Monitor your product and service suppliers to become aware of cybersecurity incidents.
II. Continuously monitor and document risks associated with your product and service suppliers.
III. Reassess risks associated with your product and service suppliers routinely and as needed.

PLAN ELEMENTS

TABLE 1: RESOURCE MAPPING

Plan Elements	Acquirer	Integrator	Supplier
1. **Begin with An Executive Summary** 2. **Identify Supply Chain Risks To Your Critical Assets** 3. **Identify Critical Suppliers** 4. **Implement Supplier Diversity** 5. **Develop A Vendor Attestation Process** 6. **Develop A Contingency Plan** 7. **Train Your Employees** 8. **Continuously Monitor And Improve**	• NIST Cybersecurity Framework Version 1.1 • NIST Special Publication 800-161R1 • NISTIR 8276 Key Practices In Cyber Supply Chain Risk Management • Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks	• NIST Cybersecurity Framework Version 1.1 • NIST Special Publication 800-161R1 • NISTIR 8276 Key Practices In Cyber Supply Chain Risk Management • Federal Acquisition Security Council Final Rule • EO 13873 Securing the ICT and Services Chain • Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks	• Federal Acquisition Security Council (FASC) Final Rule • EO 13873 Securing the ICT and Services Chain • Operationalizing the Vendor SCRM Template for Small and Medium-Sized Businesses • Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks

The resources included in Table 1 are those that were primarily used to inform the plan elements listed in this guide. Although the resources can be applied to all plan elements, the resources listed in the respective columns are especially useful if your organization falls under one of these roles. A full list of supporting resources is also included in Appendix A.

APPENDIX A: SUPPORTING RESOURCES

Primary Resources:

- NIST Cybersecurity Framework Version 1.1

  "The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes".

- NIST Special Publication 800-161

  The purpose of this publication is to provide "...guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations".

- NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management

  "This document provides the ever-increasing community of digital businesses a set of Key Practices that any organization...", regardless of size, scope, or complexity, "...can use to manage cybersecurity risks associated with their supply chains".

- Federal Acquisition Security Council Final Rule

  This rule, which was promulgated pursuant to the Federal Acquisition Supply Chain Security Act of 2018 implements "...requirements of the laws that govern the operation of the FASC, the sharing of supply chain risk information, and the exercise of the FASC's authorities to recommend issuance of removal and exclusion orders to address supply chain security risks".

- Federal Communications Commission Covered List

  "...a list of communications equipment and services (Covered List) that are deemed to pose an unacceptable risk to the national security of the United States or the security and safety of United States persons...".

- Operationalizing the Vendor SCRM Template for Small and Medium-Sized Businesses

  Provides a set of questions regarding an ICT supplier/provider's implementation and application of industry standards and best practices that can help small and medium-sized businesses guide supply chain risk planning in a standardized way.

- Securing Small and Medium-Sized Business (SMB) Supply Chains: A Resource Handbook to Reduce Information and Communication Technology Risks

  This handbook provides an overview of the highest supply chain risk categories commonly faced by ICT small and medium-sized businesses (SMBs), including cyber risks, and resources that can assist SMBs.

Secondary Resources and Executive Orders (EO):

- CISA: Secure by Design
- OMB Memorandum M-23-16
- SECURE Technology Act: Establishment of the Federal Acquisition Security Council
- Federal Acquisition Supply Chain Security Act graphic
- H.R.7327 SECURE Technology Act
- DNI ICD 731 Supply Chain Risk Management for the Intelligence Community
- DNI ICS 731-01 Supply Chain Criticality Assessment 20151002
- DNI ICS 731-02 Supply Chain Threat Assessments 20160517
- DNI ICS 731-03 Supply Chain Information Sharing
- DNI ICS 731-04 Supply Chain Vulnerability Assessments
- DNI ICS 731-05 Supply Chain Risk Assessments
- NIST: Security Measures for "EO-Critical Software" Use
- NIST: Software Supply Chain Security Guidance Under Executive Order (EO) 14028
- EO 13636 Improving Critical Infrastructure Cybersecurity
- EO 13806 Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain

APPENDIX A: SUPPORTING RESOURCES

Resiliency of the United States
- EO 13873 Securing the Information and Communications Technology and Services Supply Chain
- Executive Order 13806 Report
- EO 13913 Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector
- EO 13984 Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities
- EO 14005 Ensuring the Future Is Made in All of America by All of America's Workers
- EO 14017 America's Supply Chains
- EO 14024 Blocking Property with Respect to Specified Foreign Activities of the Government of the Russian Federation
- EO 14028 Improving the Nation's Cybersecurity
- EO 14034 Protecting Americans' Sensitive Data from Foreign Adversaries

APPENDIX B: CONTRIBUTING PARTICIPANTS

Leadership Team	Name	Organization
Co-Chair	Ola Sage	CyberRx
Co-Chair	Jeffery Goldthorp	Federal Communications Commission
Co-Chair	Tamber Ray	NTCA - The Rural Broadband Association

Writing Team Participants

Name	Organization
Andras Szakal	The Open Group
Bob Dix	Acquisition Advisory Council (AAC)
Chad Kliewer	ISC^2
Christopher Calfee	Federal Deposit Insurance Corporation (FDIC)
Dick Brooks	Reliable Energy Analytics
Frank Bulk	Premier Communications
Jerry Horton	Blue Valley Technologies, Inc.
John Bienko	Small Business Administration (SBA)
Justin Storms, Karen Keating	Federal Energy Regulatory Commission (FERC)
Kathryn Basinsky, Megan Doscher	National Telecommunications and Information Administration (NTIA)
Larry Walke	National Association of Broadcasters (NAB)
Leanna Wade	ActOnline
Matt Oyer	National Association of State Procurement Officials (NASPO)
Melissa Newman	Telecommunications Industry Association (TIA)
Rebecca Adams, Briana Alston, Amanda Ingram	DHS CISA

DHS POINT OF CONTACT

National Risk Management Center
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
NRMC@hq.dhs.gov
For more information about NRMC, visit https://www.cisa.gov/about/divisions-offices/national-risk-management-center