



Developing a Resilient SCRM Plan For Small and Medium-Sized Businesses



OVERVIEW

For many information and communications technology (ICT) small and medium-sized businesses (SMBs), a crucial element for success is the development and implementation of a supply chain risk management (SCRM) plan. Implementing a thorough SCRM plan not only provides guidance for responding to supply chain disruptions, it can also enhance an organization’s overall resiliency. SCRM plans can help grant recipients and vendors comply with the requirements of federal grants and government procurement processes. The ICT Supply Chain Risk Management Task Force developed the *Empowering SMBs: A Resource Guide For Developing a Resilient Supply Chain Risk Management Plan* to help SMBs develop and tailor an ICT SCRM plan that meets the needs of their business. Although primarily focused on the ICT sectors, this guide is relevant for SMBs in any industry.

KEY SCRM PLAN ELEMENTS

This resource guide contains eight essential steps to create a SCRM plan that an SMB can follow in order to best mitigate supply chain risks throughout their organization. These steps include:

Table 1: Plan Elements

Element	Guidance Summary
1. BEGIN WITH AN EXECUTIVE SUMMARY	Create a brief executive summary that includes a high-level overview of the purpose, goals, objectives and key elements of the plan.
2. IDENTIFY CRITICAL SUPPLIERS	Identify the suppliers that have access to or provide hardware or software, including cloud services, to your business.
3. IDENTIFY SUPPLY CHAIN RISKS TO YOUR CRITICAL ASSETS	Identify supply chain risks to better understand which critical assets and/or suppliers, if disrupted or compromised, will negatively impact your business operations.
4. IMPLEMENT SUPPLIER DIVERSITY	Maintain a diverse supplier base when possible to reduce dependence on any one supplier as relying on a single critical supplier can increase risk if critical products or services become unavailable.
5. DEVELOP A VENDOR ATTESTATION PROCESS	Evaluate vendors prior to making a purchase and maintain supplier quality over time by implementing processes and documentation by which suppliers attest, at the outset and regularly thereafter, to specific risk management attributes.
6. DEVELOP A CONTINGENCY PLAN	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.

7. TRAIN YOUR EMPLOYEES	Train employees on ICT SCRM best practices to ensure that they understand the importance of managing supply chain risks and their roles in the process.
8. CONTINUOUSLY MONITOR AND IMPROVE	Continuously monitor and improve the SCRM program to ensure the content remains effective and relevant to business operations.

Key Roles an SMB Can Assume

ICT SMBs often perform different roles in the course of conducting their business. Accordingly, organizations will need to 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.

RESOURCES

- ICT Supply Chain Risk Management Task Force: [CISA.gov/ict-scrm-task-force](https://cisa.gov/ict-scrm-task-force)
- ICT Supply Chain Library: [CISA.gov/ict-supply-chain-library](https://cisa.gov/ict-supply-chain-library)
- ICT SCRM Task Force Resources: [CISA.gov/ict-scrm-task-force-resources](https://cisa.gov/ict-scrm-task-force-resources)

For more information or to seek additional help, contact us at NRMC@hq.dhs.gov.

