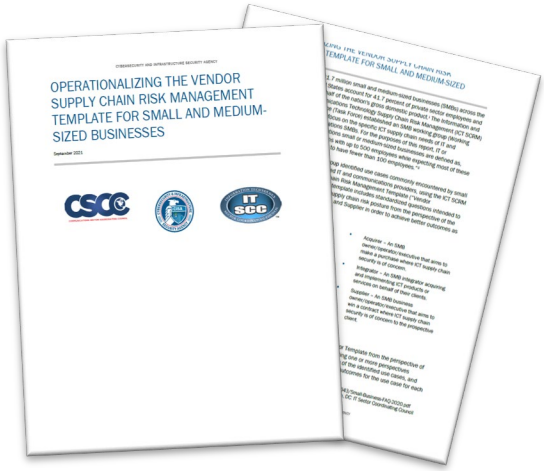
IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

ASSISTING SMALL AND MEDIUM-SIZED BUSINESSES ASSESS VENDORS AND SUPPLIERS

OVERVIEW



With more than 30 million small and medium-sized businesses (SMBs) across the United States, they account for nearly half of the nation's gross domestic product. Many of them depend on suppliers and other business partners to stay in business and therefore should be aware of the cybersecurity threats that can impact their information and communications technology (ICT) supply chain. Protecting their supply chains requires a combination of layered defenses. The Cybersecurity and Infrastructure Security Agency's (CISA) ICT Supply Chain Risk Management (SCRM) Task Force developed the Operationalizing the Vendor Supply Chain Risk Management Template for Small and Medium-Sized Businesses (Guide) to help SMBs assess the security posture of their vendors and suppliers. The guide provides a set of questions with step-by-step guidance to help organizations conduct standardized supply chain risk planning when purchasing ICT hardware, software, and services.

MEETING THE UNIQUE NEEDS OF SMBS

The ICT SCRM Task Force recognizes the need for guidance that would be practical, accessible, and usable by the SMB community. The guide details three use cases commonly encountered by IT and Communications-sector SMBs and selected questions for each of these use cases directly from the ICT SCRM Task Force's Vendor SCRM Template that are most relevant to SMBs. The questions can be used to help understand ICT supply chain risks from the perspective of the SMB as the acquirer, integrator, or supplier to achieve enhanced outcomes. These roles can be defined as:

- **Acquirer:** An SMB owner/operator/executive that aims to make a purchase where ICT supply chain security is of concern.
- **Integrator:** An SMB integrator acquiring and implementing ICT products or services on behalf of their clients.
- **Supplier:** An SMB business owner/operator/executive that aims to win a contract where ICT supply chain security is of concern to the prospective client.

Table 1: Use Cases

Use Case #	Use Case Title	Use Case Description
Use Case 1	Applying ICT Vendor SCRM to Physical or Logical Access Controls	Focuses on the risk that is introduced whenever an SMB permits physical or logical access to facilities or systems.
Use Case 2	Applying Vendor SCRM To Cloud-Hosted Solutions	Addresses the use of cloud-hosted solutions that are essential to the SMB's business operations, including business collaboration productivity suites, customer relationship management tools, and credit card processing.

Use Case 3	Vetting Managed Service Providers (MSPs)	Creates a template to help SMBs vet Managed Service Providers (MSP) that will have critical access to the SMBs systems or data.

If an SMB is utilizing multiple use cases, it may be helpful to identify common questions among them. Answers to these multiple questions might rest somewhere between *yes* and *no*. As a result, the guide includes an accompanying easy-to-use spreadsheet as an alternate tool for organizations to answer the same questions selected for each use case.

Table 2: Accompanying Spreadsheet

Question	Responses (Yes, No, Partial)	Explain "Partial" Responses
1.1 Have you previously provided supply chain risk management information to this organization? If "yes", please provide an updated revision covering material changes.		
OR		
1.2 Do you have controls fully aligned to NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organization?		
If you responded affirmatively to ANY of the questions above, you may attach supporting documentation and skip the remaining questions.		
3.17. Does your organization analyze vulnerabilities to identify root cause?		
4.3. Do you have company-wide, publicly available information security policies in place covering privacy policies?		
4.7. Do you have an asset management program approved by management for your IT assets that is regularly maintained?		
4.10. Do you have documented hardware and software policies and practices in place to ensure asset integrity?		
4.15. Do you have network access control policies and procedures in place for your information systems that are aligned with industry standards or control frameworks?		
4.16. Is cybersecurity training required for personnel who have administrative rights to your enterprise computing resources?		
4.17. Do you include contractual obligations to protect information and information systems handled by your suppliers?		
4.19. Does your organization have hardening standards in place for network devices (e.g., wireless access points, firewalls, etc.)?		
4.21. Do you have defined and documented incident detection practices that outline which actions should be taken in the case of an information security or cybersecurity event?		
4.26. Do you have processes or procedures to recover full functionality, including integrity verification, following a major cybersecurity incident?		

RESOURCES

- ICT Supply Chain Risk Management Task Force: CISA.gov/ict-scrm task-force