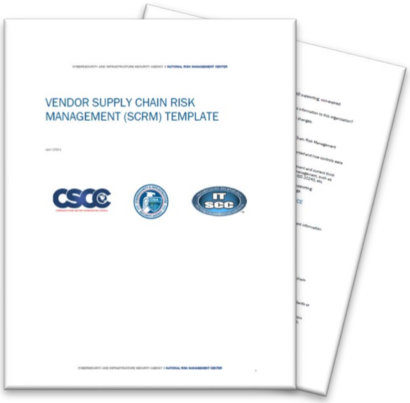
IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

PROCURING SAFE AND SECURE ICT PRODUCTS AND SERVICES

DEFEND TODAY,
SECURE TOMORROW



CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY I NATIONAL RISK MANAGEMENT CENTER

VENDOR SUPPLY CHAIN RISK MANAGEMENT (SCRM) TEMPLATE

April 2021

OVERVIEW

Protecting your organization’s data requires understanding not only your immediate supply chain, but also your vendors' and suppliers' supply chain practices. The Cybersecurity and Infrastructure Security Agency’s (CISA), Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force developed a Vendor SCRM Template to help organizations and businesses of any size assess the security posture of their vendors and suppliers in a standard way when purchasing ICT hardware, software, and services.

ASSESSING VENDOR AND SUPPLIER TRUSTWORTHINESS

Having trustworthy vendors and suppliers are key elements to manage and reduce supply chain risks. The Vendor SCRM Template is a baseline questionnaire to help organizations address potential gaps in their supply chain procurement process. It builds upon existing industry standards to enable both vendors and customers to communicate in a way that is consistently understood, predictable, and actionable. These questions provide enhanced visibility and transparency into entity trust and assurance practices and assist in informed decision-making about acceptable risk exposure. The template can help enhance any organization’s supply chain risk posture and resiliency by ensuring that purchased products meet industry standards.

The questions listed in Table 1 are grouped in seven key categories, broadly covering ICT supply chain risk management, governance, and associated risk domains. The seven key categories are: Supply Chain Management and Supplier Governance, Secure Design and Engineering, Information Security, Physical Security, Personnel Security, Supply Chain Integrity, and Supply Chain Resilience.

Table 1: Vendor SCRM Template Sample Questions

Category	Sub-Category	Sample Question
1. Supply Chain Management and Supplier Governance	ICT Supply Chain Management	Do you have a documented Quality Management System for your ICT supply chain operation based on an industry standard or framework?
2. Secure Design and Engineering	Product Offering Lifecycle Management and Organization	Does your organization document and communicate security control requirements for your hardware, software, or solution offering?
3. Information Security	Asset Management	Do you inventory and audit back-up, replacement hardware, and software assets to ensure their accountability and integrity?
4. Physical Security	Physical Security in Transit	Do you utilize a controlled bill of materials or similar capability to protect assets that are being received, in process, or in-transit?
5. Personnel Security	Onboarding	Do you have a process for onboarding personnel?

6. Supply Chain Integrity	Supply Chain Integrity	Do you have documented performance and validation procedures for your hardware/software products or services?
7. Supply Chain Resilience	Diversity of Supply Base	Does your company consider supplier diversity to avoid single sources and to reduce the occurrence of suppliers being susceptible to the same threats to resilience?

The purpose of the template is to illuminate the risk factors, so the acquiring organization understands how the risk profile of the entity aligns with their tolerance of risk for the specific product or service being provided. These questions will aid in mitigating (not eliminating) risk and are consistent with commercial and public sector standards. The questions should be used as applicable, depending on the product or service and the customer involved (*e.g.,* Department of Defense (DoD), civilian, commercial).

ROBUST METHODOLOGY

These seven key categories were built on a framework of established industry standards and other ICT SCRM Task Force efforts, while incorporating inputs from the National Institute of Standards and Technology (NIST) SP 800-161, DoD Cybersecurity Maturity Model Certification (CMMC), and the Outsourcing Network Services Assessment Tool (ONSAT).

RESOURCES

- ICT Supply Chain Risk Management Task Force: CISA.gov/ict-scrm task-force
- Operationalizing the Vendor Supply Chain Risk Management Template for Small and Medium-Sized Businesses: CISA.gov/sites/default/files/publications/ict-scrm-task-force_smb-operationalizing-vendor-template_508.pdf