NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

# NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)


U.S. Department of Commerce
*Gina M. Raimondo, Secretary*
National Institute of Standards and Technology
*Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology*

**NIST Special Publication**
**NIST SP 1305 ipd (Initial Public Draft)**
https://doi.org/10.6028/NIST.SP.1305.ipd
The public comment period for this draft ends May 3, 2024.
Please send your comments to cyberframework@nist.gov.
February 2024

# NIST CSF 2.0: CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

## A QUICK START GUIDE

## INTRODUCTION TO C-SCRM

### C-SCRM Overview

All types of technology rely on a complex, globally distributed, extensive, and interconnected supply chain ecosystem. ***Cybersecurity Supply Chain Risk Management (C-SCRM)*** is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures.

C-SCRM practitioners **identify, assess, and mitigate cybersecurity risks throughout the supply chain at all levels of their organizations** associated with information and communications technology (ICT) products and services. Potential risks include malicious functionality, counterfeit devices, or vulnerabilities derived from poor manufacturing and development practices within the supply chain.

Effective C-SCRM requires stakeholders across the enterprise to **actively collaborate, communicate, and take actions** to secure favorable C-SCRM outcomes.

**This Quick-Start Guide provides an overview of C-SCRM and how it relates to the Cybersecurity Framework (CSF). Organizations implementing C-SCRM capabilities should not rely solely on this QSG and should consult the additional documents referenced within.**

### Use the CSF to Improve Your C-SCRM Processes

The CSF can help an organization become a smart acquirer and supplier of technology products and services. This guide focuses on two ways the CSF can help you:

1. **Use the CSF's GV.SC Category to establish and operate a C-SCRM capability.**
2. **Define and communicate supplier requirements using the CSF.**

#### What is the supply chain ecosystem?

The ***supply chain ecosystem*** is composed of public and private sector entities — including acquirers, suppliers, developers, system integrators, external system service providers, and other technology-related service providers — that interact to research, develop, design, manufacture, acquire, deliver, integrate, operate, maintain, dispose of, and otherwise utilize or manage technology products and services.

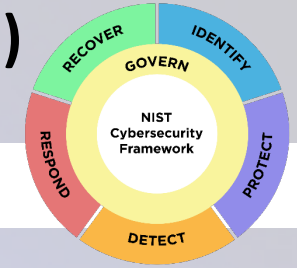
Consider a laptop with hardware subcomponents (like the graphics processor, random-access memory, or network interface card) sourced from different countries and third-party manufacturers, and subject to distinct supply chain interactions. That laptop also contains software (and firmware) developed by different companies and people. How do we manage risk for complex ICT devices with multiple components?

In today's interconnected world, the supply chain ecosystem includes other third parties such as business partners and various data and digital service providers. Practices in this QSG can be applied to manage cybersecurity risks from such relationships as well.

# NIST CSF 2.0: CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

## A QUICK START GUIDE

## HOW TO USE THE CSF TO ESTABLISH AND OPERATE A C-SCRM CAPABILITY




### Establishing a C-SCRM Capability

The CSF has a Category within its Govern Function dedicated to C-SCRM: the Cybersecurity Supply Chain Risk Management (GV.SC) Category. GV.SC contains the key outcomes that every organization should achieve through its C-SCRM capability. Additionally, many of the subcategories within the remainder of the CSF can be used to identify and communicate C-SCRM-related requirements internally for organizations and for their vendors.

**Perform these activities to establish your organization's C-SCRM capability:**

**Activity 1: Create a C-SCRM strategy, objectives, policies, and processes.** [GV.SC-01]

**Activity 2: Identify your organization's technology suppliers and determine how critical each one is to your organization.** [GV.SC-04]

**Activity 3: Establish C-SCRM roles and requirements and communicate them within and outside your organization.** This includes identifying C-SCRM roles and responsibilities [GV.SC-02] and C-SCRM requirements [GV.SC-05].

**It is also important to coordinate and harmonize activities between your C-SCRM capability and other internal capabilities. Here are a few examples:**

- Integrate C-SCRM into cybersecurity and enterprise risk management, risk assessment, and improvement processes, and monitor the performance of C-SCRM practices throughout the technology lifecycle. [GV.SC-03, GV.SC-09] See the *Enterprise Risk Management Quick-Start Guide* for more information on C-SCRM integration.
- Include your relevant suppliers in cybersecurity incident planning, response, and recovery activities. [GV.SC-08] See NIST's *Computer Security Incident Handling Guide* for more information on key practices for cybersecurity incidents.

### Checklist of actions for Activity 1: Create a C-SCRM strategy, objectives, policies, and processes.

- ☐ Establish a C-SCRM strategy that lays out the objectives of the capability.
- ☐ Develop a C-SCRM plan (with milestones) and C-SCRM policies and procedures that guide implementation and improvement of the plan and the capability; socialize those policies and procedures with organizational stakeholders.
- ☐ Develop and implement C-SCRM processes based on the strategy, objectives, policies, and procedures that are agreed upon and performed by the organizational stakeholders.
- ☐ Establish a cross-organizational mechanism that ensures alignment between functions that contribute to C-SCRM management, such as cybersecurity, IT, legal, human resources, engineering, etc.

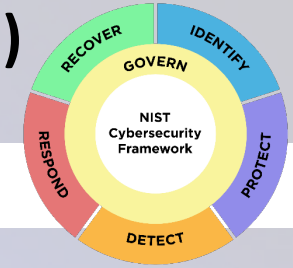
### Checklist of actions for Activity 2: Identify your organization's technology suppliers and determine how critical each one is to your organization.

- ☐ Develop criteria for supplier criticality based on, for example, the importance of the supplier's products or services to the organization's business, sensitivity of data processed or stored by the supplier, and degree of access to the organization's systems.
- ☐ Prioritize suppliers into criticality levels based on the criteria. See NIST IR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components* for more information on a structured method for prioritization.
- ☐ Keep a record of all suppliers, prioritized based on the criticality criteria.

# NIST CSF 2.0: CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

## A QUICK START GUIDE

## HOW TO USE THE CSF TO ESTABLISH AND OPERATE A C-SCRM CAPABILITY




### Checklist of actions for Activity 3: Establish C-SCRM roles and requirements and communicate them within and outside your organization.

#### C-SCRM roles and responsibilities:

- ☐ Identify one or more specific roles or positions that will be responsible and accountable for planning, resourcing, and executing C-SCRM activities.
- ☐ Document C-SCRM roles and responsibilities in policy.
- ☐ Create responsibility matrixes (e.g., RACI charts) to document who will be responsible, accountable, consulted, and informed for C-SCRM activities and how those teams and individuals will be consulted and informed.
- ☐ Include C-SCRM responsibilities and performance requirements in personnel descriptions to ensure clarity and improve accountability.
- ☐ Document performance goals for personnel with C-SCRM responsibilities, and periodically measure them to demonstrate and improve performance.
- ☐ Develop roles and responsibilities for suppliers, customers, and business partners to address shared responsibilities for applicable cybersecurity risks and integrate them into organizational policies and applicable third-party agreements.
- ☐ Internally communicate C-SCRM roles and responsibilities for suppliers.
- ☐ Establish rules and protocols for information sharing and reporting processes between the organization and its suppliers.

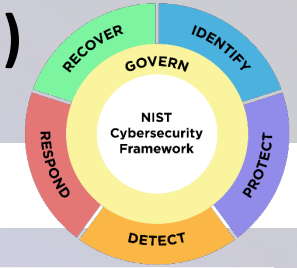
#### C-SCRM requirements:

- ☐ Establish security requirements for suppliers, products, and services commensurate with their criticality and potential impact if compromised.
- ☐ Include all cybersecurity and supply chain requirements that suppliers must follow and how compliance with the requirements may be verified in default contractual language.
- ☐ Define the rules and protocols for information sharing between the organization and its suppliers and sub-tier suppliers in contracts.
- ☐ Include security requirements in contracts based on their criticality and potential impact if compromised.
- ☐ Define security requirements in service level agreements (SLAs) for monitoring suppliers for acceptable security performance throughout the supplier relationship lifecycle.
- ☐ Specify in contracts the rights and responsibilities of the organization, its suppliers, and their supply chains with respect to potential cybersecurity risks. Contractually require suppliers to do the following:
  - ☐ disclose cybersecurity features, functions, and vulnerabilities of their products and services for the life of the product or the term of service
  - ☐ provide and maintain a current component inventory (e.g., software or hardware bill of materials) for critical products
  - ☐ vet their employees and guard against insider threats
  - ☐ provide evidence of performing acceptable security practices through, for example, self-attestation, conformance to known standards, certifications, or inspections

# NIST CSF 2.0: CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

## A QUICK START GUIDE

## HOW TO USE THE CSF TO DEFINE AND COMMUNICATE SUPPLIER REQUIREMENTS




### Developing Supplier Requirements

An organization should specify requirements for technology suppliers. Robustness of these requirements should correspond to supplier criticality.

Organizations can use two different methods for specifying supplier requirements:

1. **Use CSF Categories and Subcategories.** Not all Categories and Subcategories will apply to all suppliers. You can pick and choose requirements that fit your mission or business supplier criticality level. Select requirements for suppliers based on their criticality and your mission or business. To do that, review the list of CSF Categories and Subcategories, and determine which ones will be applicable to suppliers within each of the criticality levels, based on the risk appetite for each supplier criticality level.

When considering individual supplier agreements, determine if additional supplier requirements are needed based on existing criticality criteria, such as your mission or business, data type being processed, or digital product or service being provided.

**2. Create CSF Target Profiles for Each Supplier Criticality Level.** The next page explains how to express supplier requirements for each supplier criticality level.

### Examples of CSF Categories and Subcategories that are likely to include requirements for suppliers

#### Govern:

- **Organizational Context:** Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed [GV.OC-03]
- **Roles, Responsibilities, and Authorities:** Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced [GV.RR-02]
- **Cybersecurity Supply Chain Risk Management:** Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders [GV.SC]

#### Identify:

- **Risk Assessment:** The authenticity and integrity of hardware and software are assessed prior to acquisition and use [ID.RA-09]; Critical suppliers are assessed prior to acquisition [ID.RA-10]
- **Improvement:** Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties [ID.IM-02]

#### Protect:

- **Identity Management, Authentication, and Access Control:** Identities and credentials for authorized users, services, and hardware are managed by the organization [PR.AA-01]
- **Awareness and Training:** Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind [PR.AT-02]

#### Detect:

- **Continuous Monitoring:** Personnel activity and technology usage are monitored to find potentially adverse events [DE.CM-03]

#### Respond:

- **Incident Management:** Incidents are escalated or elevated as needed [RS.MA-04]
- **Incident Response Reporting and Communication:** Internal and external stakeholders are notified of incidents [RS.CO-02]

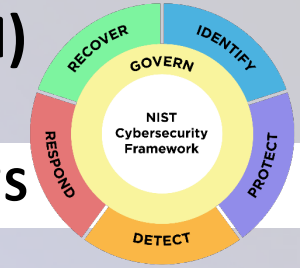
#### Recover:

- **Incident Recovery Plan Execution:** The integrity of backups and other restoration assets is verified before using them for restoration [RC.RP-03]
- **Incident Recovery Communication:** Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders [RC.CO-03]

# NIST CSF 2.0: CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

## A QUICK START GUIDE

## HOW TO USE THE CSF TO DEFINE AND COMMUNICATE SUPPLIER REQUIREMENTS




### Create Target Profiles to Communicate Supplier Requirements by Supplier Criticality Level

**Follow these steps to create Target Profiles for communicating C-SCRM requirements to your suppliers.**

1. **Scope the Target Profile.** Decide which of your supplier criticality levels it will apply to, and determine any other restrictions to be placed on the Profile's scope, such as suppliers of a particular type of product or service only. You can create as many Target Profiles as you need to specify the requirements for all of your suppliers.
2. **Select the CSF Categories to include.** Identify which CSF Categories and Subcategories correspond to your requirements, and only include those Categories and Subcategories in the Target Profile.
3. **Determine what types of information to include in your Target Profile.** Target Profiles are flexible and can contain whatever types of information you want to communicate to your suppliers. The notional Profile excerpt below captures each selected Category's and Subcategory's relative priority, the internal practices that the supplier must follow, and references to additional sources of information on achieving the Category and Subcategory.
4. **Fill in the columns, and share the Target Profile.** Once the contents of the Target Profile have been internally reviewed and finalized, it can be shared with your suppliers as your set of C-SCRM requirements for them.

| Selected CSF Outcomes | Target Priority | Target Internal Practices | Selected Informative References |
|---|---|---|---|
| PR.PS, The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability | High | 1. Configure platforms to allow the installation of organization-approved software only.<br>2. Verify the source of new software and the software's integrity before installing it.<br>3. Configure platforms to use only approved DNS services that block access to known malicious domains.<br>4. … | • NIST SP 800-161r1, control SI-3<br>• ISO 27002:2022, control 8.7<br>• … |
| … | | | |

### Additional resources for creating Target Profiles

- *Quick-Start Guide for Creating and Using Organizational Profiles* (including Target Profiles)
- *A Guide to Creating CSF 2.0 Community Profiles* (Community Profiles have much in common with creating Target Profiles for numerous suppliers to follow)
- *Quick-Start Guide for Using the CSF Tiers* (to help inform creation of Target Profiles)
- *Enterprise Risk Management Quick-Start Guide*
- *Informative Reference Mapping Quick-Start Guide* (for accessing and using existing Informative References for a Target Profile)

# NIST CSF 2.0: CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

## A QUICK START GUIDE

## NEXT STEPS

**What We Learned.** This QSG explained the following:

**What Is C-SCRM** – a systematic process for managing exposure to cybersecurity risk throughout supply chains

**What Is a Supply Chain Ecosystem** – public- and private-sector entities that interact to create, deliver, operate, and manage technology products and services

**How to Establish and Implement a C-SCRM Capability** – by using the CSF 2.0 C-SCRM Category (GV.SC)

**How to Develop Supplier Requirements** – by using the CSF Categories and Subcategories or by creating Target Profiles

**What's Next.** Here's a list of things you can do to move this QSG into practice:

- Review all NIST CSF 2.0 Categories and Subcategories
- Develop C-SCRM strategy, objectives, policies, and processes [**Activity 1**]
- Identify your organization's technology suppliers [**Activity 2**]
- Determine how critical each technology supplier is to your organization and prioritize your suppliers [**Activity 2**]
- Establish C-SCRM roles and requirements [**Activity 3**]
- Communicate C-SCRM roles and requirements within and outside your organization, including to technology suppliers [**Activity 3**]

**This QSG provides an overview of C-SCRM and how it relates to the CSF. Organizations implementing C-SCRM capabilities should not rely solely on this QSG and should consult the additional documents referenced within.**

## New to C-SCRM?

Here are some NIST resources that can help you get up to speed on the basics of C-SCRM and support you in establishing and operating your C-SCRM capability:

- *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* (NIST IR 8276) summarizes practices foundational to an effective C-SCRM capability.
- *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (NIST SP 800-161 Revision 1) guides organizations in identifying, assessing, and responding to supply chain risks at all levels. It is flexible and builds on an organization's existing cybersecurity practices. Also, Appendix A identifies the C-SCRM-related controls from NIST SP 800-53r5 and augments those controls with additional supplemental guidance, as well as providing new controls as appropriate.
- *Criticality Analysis Process Model: Prioritizing Systems and Components* (NIST IR 8179) provides information on prioritizing suppliers by criticality levels.
- The Software and Supply Chain Assurance Forum provides a venue for government, industry, and academic participants from around the world to share their knowledge and expertise regarding C-SCRM, supply chain risks, effective practices and response strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved.
- NIST's C-SCRM Program website contains links to additional resources.