3
4 # Cyber Supply Chain Risk Management Practices for Systems and Organizations
5

6
7
8 Jon Boyens
9 Angela Smith
10 Nadya Bartol
11 Kris Winkler
12 Alex Holbrook
13 Matthew Fallon
14
15
16
17
20

**NIST**

**National Institute of Standards and Technology**
U.S. Department of Commerce

# Cyber Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
*Computer Security Division*
*Information Technology Laboratory*

Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon
*Boston Consulting Group*

## Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

**Public comment period: *April 29, 2021* through ~~*June 14*~~ *June 25, 2021***

All comments are subject to release under the Freedom of Information Act (FOIA).

96                     **Reports on Computer Systems Technology**

97    The Information Technology Laboratory (ITL) at the National Institute of Standards and
98    Technology (NIST) promotes the U.S. economy and public welfare by providing technical
99    leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test
100   methods, reference data, proof of concept implementations, and technical analyses to advance the
101   development and productive use of information technology. ITL's responsibilities include the
102   development of management, administrative, technical, and physical standards and guidelines for
103   the cost-effective security and privacy of other than national security-related information in federal
104   information systems. The Special Publication 800-series reports on ITL's research, guidelines, and
105   outreach efforts in information system security, and its collaborative activities with industry,
106   government, and academic organizations.
107

108                              **Abstract**

109   Organizations are concerned about the risks associated with products and services that may
110   contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor
111   manufacturing and development practices within the cyber supply chain. These risks are
112   associated with an enterprise's decreased visibility into, and understanding of, how the
113   technology that they acquire is developed, integrated, and deployed, as well as the processes,
114   procedures, and practices used to assure the security, resilience, reliability, safety, integrity, and
115   quality of the products and services.
116

117   This publication provides guidance to organizations on identifying, assessing, and mitigating
118   cyber supply chain risks at all levels of their organizations. The publication integrates cyber
119   supply chain risk management (C-SCRM) into risk management activities by applying a multi-
120   level, C-SCRM-specific approach, including guidance on development of C-SCRM strategy
121   implementation plans, C-SCRM policies, C-SCRM plans, and C-SCRM risk assessments for
122   products and services.

123                              **Keywords**

127
128

129                                **Acknowledgements**

140
141                                **Note to Reviewers**
142
143   Revision 1 of this foundational NIST publication represents a one-year effort to incorporate the
144   next generation C-SCRM controls that will be needed to accomplish the above objectives. It
145   includes changes to make the SP more modular based, expand alignment to [NIST 800-37], *Risk*
146   *Management Framework for Information Systems and Organizations: A System Life Cycle*
147   *Approach for Security and Privacy* as well as NIST [800-39], *Managing Information Security*
148   *Risk: Organization, Mission, and Information System View*. Changes also focus on making
149   implementation guidance more consumable by acquirers, suppliers, developers, system
150   integrators, external system service providers, and other ICT/OT-related service providers as
151   well as increasing enablement through the inclusion of C-SCRM Strategy & Implementation
152   Plan, C-SCRM Policy, C-SCRM Plan, and Cyber Supply Chain Risk Assessment templates.
153
154   Questions to reviewers:
155
156   •   Does this document strike the right balance with respect to providing guidance any
157       organization can use, regardless of size, mission, etc., and providing guidance sufficiently
158       descriptive to be clear and actionable?
159   •   Does this guidance offer organizations a structure both easy to follow and
160       implement??  If not, how could the guidance be structured, the content be represented,
161       and main points/concepts be highlighted so that the user can build a C-SCRM program
162       and capabilities using the minimum amount of time and resources?
163   •   Is anything missing in the implementation guidance that you would have expected to see?
164       Is there any guidance that is not needed?
165   •   Within Section 3.1.1 – Acquisition in the C-SCRM Strategy & Implementation Plan, are
166       we providing the right balance of guidance?
167   •   Within Section 3.4 – Is one implementation model preferred versus the other? Or both?
168       Or is there a different approach preferred that is not currently reflected?
169       Within Section 3.4.1 – Is the document providing the right balance and mix of
170       capabilities across the Foundational, Sustaining, and Enhancing practice categories?
171   •   Within Appendix D 4.1 Cyber Supply Chain Risk Assessment Template – What can
172       improve the product or service assessment? Should it be combined with a supplier

173    assessment? What should be asked of the supplier? Should the assessment ask about the
174    technology being acquired?
175
176    Major changes include:
177
178    • Updated diagrams and tables throughout
179
180    Additional major changes per section / appendix include:
181
182    Section 1, Introduction
183    • Refined cyber supply chain risk management definition to include internal and external
184      dependency considerations to improve clarity.
185    • Clarified and expanded upon the meanings of the C-SCRM products, services (e.g.,
186      Human Resources, Payroll, Cloud Providers, and Managed Security), and supply chain
187      elements.
188    • Incorporated types of factors that are associated with services that drive risk
189      identification, assessment and response considerations.
190    • Described relationship between traditional supply chain (e.g., Supply Chain Operations
191      Reference) and C-SCRM. Established NIST C-SCRM as the authoritative definition.
192    • Expanded scope from High Impact Systems to High, Moderate, and Low Impact
193      Systems, per draft SP 800-53B (baselines); included Operational Technology (OT) and
194      Internet of Things (IoT) considerations throughout.
195    • Added of *Section 1.3, The Business Case for C-SCRM*, and *Section 1.7 Implementing C-*
196      *SCRM* in the context of SP 800-37 Rev. 2.
197    • Updated the regulatory, legislative, and guidance references to include developments
198      since initial publication (e.g., SP 800-160, SP 800-53 Rev. 5, SECURE Technology Act
199      of 2018, etc.).
200    • Acknowledgement of C-SCRM as a multidisciplinary topic that demands coordination
201      across multiple disciplines (e.g., acquisition policy/management, logistics management,
202      legal, and intelligence).
203    • Defined C-SCRM relational boundaries (e.g., National Security Systems, High Value
204      Assets, Critical Infrastructure, and Government-as-Enterprise).
205
206    Section 2, Integration of C-SCRM into Organization-wide Risk Management
207    • Movement of Frame, Assess, Respond, Monitor (FARM) processes to Appendix C
208    • C-SCRM Program Management:
209        o Defined the scope and characteristics of a C-SCRM Program across
210          organizational tiers.
211        o Introduced the concepts of a dedicated C-SCRM PMO within one or more
212          organizational tiers and codify the C-SCRM PMO's purpose, high-level roles and
213          responsibilities, and scope of responsibilities.
214        o Explored models of vertical and horizontal coordination across organizational
215          tiers, especially where numerous PMO responsibilities may overlap (e.g.,
216          facilitate matrix management and coordination of disparate discipline-area
217          specific SCRM functions, enable governance and integration with enterprise risk

218      management, liaise with external entities/officials, track/manage/report on SCRM
219      implementation progress and overall program effectiveness).
220      o   Consider resource and budgetary constraints via alternate operational models
221      (e.g., formal and less formal PMOs), as well as methods for how to determine the
222      model that is "fit for purpose".
223      o   Concrete guidance provided to assess and measure the effectiveness of an
224      organization's C-SCRM program capabilities and program outcomes related to
225      mitigating or otherwise appropriately managing cyber supply chain risks.
226    •   Acquisition Security:
227      o   Acquisition Security concepts (further explored in Section 3) have been added
228      across the risk framework levels.
229      o   Processes described from a Buyer's perspective (e.g., how a member of the
230      Acquisition Team can effectively evaluate the relative merits of a given
231      contractor's C-SCRM controls or their supply chain risk exposure and use that
232      information appropriately when making acquisition-related decisions). Link to
233      OMB A-123.
234    •   Implementing C-SCRM in the Context of SP 800-37 Rev. 2:
235      o   Clear linkage made with SP 800-37 Rev 2. and System Level (Level 3) C-SCRM
236      guidance.

237 *This section included the following revisions:*
238    •   Risk Management Process:
239      o   Integrated into and enhanced existing frame, assess, respond, and monitor
240      activities with the latest operational and technological trends. Improved
241      traceability of tasks with their associated infographics. Generally, expanded roles
242      and responsibilities concepts. Refined and clarified what risk tolerance means,
243      who determines it and upon what it is based, and how it is used to inform and
244      influence risk response decisions.
245      o   Discussed importance of a documented, foundational methodology that provides
246      for a repeatable and standardized way to codify risk information via SP 800-37
247      Rev. 2 and the SP 800-53 Rev. 5 SR Family.
248    •   Interdependencies:
249      o   Impact of external stakeholders, federated organizations, and other
250      interdependencies on C-SCRM was reviewed and added to as necessary.

251 Section 3, (NEW) Critical success factors
252
253 Section 4, C-SCRM Controls – *previously section three*
254    •   Updated all NIST SP 800-53 Rev. 4 mappings to NIST SP 800-53 Rev.
255    •   Updated C-SCRM controls based on SP 800-53 Rev. 5. New control sets for SR (SR-13:
256      Supplier Inventory) and MA (MA-8: Maintenance Monitoring and Information Sharing)
257      were added:
258      o   Impact System Expansion - Designated which supplemental guidance is
259      applicable to High, Moderate, and/or Low Impact Systems.

260        • Supplemental Guidance: Existing supplemental guidance was enhanced with the latest
261            operational and technological trends, and implementation guidance was added per new or
262            updated control language.

263    Appendix A – C-SCRM Control Summary
264
265    Appendix B – Risk Response Framework
266        • Changed title from Cyber Supply Chain Threat Events to Risk Response Framework.
267        • Updated language to incorporate risk-based approach.
268        • Added Scenario 1.
269        • Updated all scenarios with revised C-SCRM controls.
270
271    Appendix C – (NEW) C-SCRM ACTIVITIES IN THE RISK MANAGEMENT PROCESS
272        • Added discussion of Risk Appetite; expanded discussion of risk tolerance.
273        • Moved "FARM" from previous Section 2 to this appendix.
274
275    Appendix D – (NEW)
276        • Added C-SCRM templates to include C-SCRM Strategy and Implementation Plan, C-
277            SCRM Policy, C-SCRM Plan, and C-SCRM Risk Assessment.
278
279    Appendix E
280        • Updated to reflect updated SP 800-161 Revision 1 content to include new, changed or
281            deleted glossary terms.
282
283    Appendix F
284        • Updated to reflect updated SP 800-161 Revision 1 content to include new, changed or
285            deleted acronyms.
286
287    Appendix G
288        • Updated references to reflect new, changed or deleted references.
289
290
291    Your feedback on this draft publication is important to us. We appreciate each contribution from
292    our reviewers. The insightful comments from both the public and private sectors, nationally and
293    internationally, continue to help shape the final publication to ensure it meets the needs and
294    expectations of our customers. NIST anticipates producing the second draft of this publication in
295    September 2021 and publishing the final version no later than April 2022. These dates are
296    subject to change.
297
298
299    - JON BOYENS, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
300

301 **Call for Patent Claims**

302  This public review includes a call for information on essential patent claims (claims whose use
303  would be required for compliance with the guidance or requirements in this Information
304  Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
305  directly stated in this ITL Publication or by reference to another publication. This call also
306  includes disclosure, where known, of the existence of pending U.S. or foreign patent applications
307  relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

308  ITL may require from the patent holder, or a party authorized to make assurances on its behalf,
309  in written or electronic form, either:

310      a)  assurance in the form of a general disclaimer to the effect that such party does not hold
311          and does not currently intend holding any essential patent claim(s); or

312      b)  assurance that a license to such essential patent claim(s) will be made available to
313          applicants desiring to utilize the license for the purpose of complying with the guidance
314          or requirements in this ITL draft publication either:

315          i.   under reasonable terms and conditions that are demonstrably free of any unfair
316               discrimination; or
317          ii.  without compensation and under reasonable terms and conditions that are
318               demonstrably free of any unfair discrimination.

319  Such assurance shall indicate that the patent holder (or third party authorized to make assurances
320  on its behalf) will include in any documents transferring ownership of patents subject to the
321  assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
322  the transferee, and that the transferee will similarly include appropriate provisions in the event of
323  future transfers with the goal of binding each successor-in-interest.

324  The assurance shall also indicate that it is intended to be binding on successors-in-interest
325  regardless of whether such provisions are included in the relevant transfer documents.

326  Such statements should be addressed to: scrm-nist@nist.gov

327

**Table of Contents**

477

## 1. INTRODUCTION

478
479
480
481 Information, communications, and operational technology (ICT/OT) relies on a complex, globally distributed and interconnected supply chain ecosystem that is long, has geographically diverse routes, and consists of multiple levels of outsourcing. This ecosystem
482 is composed of public and private sector entities (e.g., acquirers, suppliers, developers, system
483 integrators, external system service providers, and other ICT/OT-related service providers)[1] and
484 technology, law, policy, procedures, and practices that interact to conduct research and
485 development, design, manufacture, acquire, deliver, integrate operate and maintain, and dispose,
486 and otherwise utilize or manage ICT/OT products and services. This ecosystem has evolved to
487 provide a set of highly refined, cost-effective, reusable solutions. Federal government
488 information systems[2] have rapidly adopted this ecosystem of solution options, which has
489 increased their reliance on commercially available products, system integrator support for
490 custom-built systems, and external service providers. This, in turn, has resulted in increased
491 complexity, diversity, and scale of the federal government's cyber supply chains.

492
493 In this document, the term ***supply chain*** refers to the linked set of resources and processes
494 between and among multiple levels of enterprises, each of which is an acquirer that begins with
495 the sourcing of products and services and extends through their life cycle.

496
497 Based on this definition, ***cyber supply chain*** is this linked set of resources that can be subject to
498 cyber supply chain risks from suppliers, their supply chains, and their products or services.
499 Cyber supply chain risks include exposures, threats, and vulnerabilities associated with the
500 products and services traversing the supply chain as well as the exposures, threats, and
501 vulnerabilities to the supply chain.

502
503 Commercially available technology solutions present significant benefits including low cost,
504 interoperability, rapid innovation, product feature variety, and the ability to choose from
505 competing vendors. These commercial off-the-shelf (COTS) solutions, whether proprietary or
506 open source, can meet the needs of a global base of public and private sector customers.
507 However, the same globalization and other factors that allow for such benefits can also increase
508 the risk of a threat event which can directly or indirectly affect the cyber supply chain—often
509 undetected—and in a manner that may result in risks to the acquirer and the end user.

510
511 These cyber supply chain risks may include but are not limited to tainted software, introduction
512 of malware, theft of intellectual property, insertion of counterfeits, unauthorized production,
513 tampering, theft, insertion of malicious software and hardware, as well as poor development and
514 manufacturing practices in the cyber supply chain. These risks are associated with an enterprise's
515 decreased visibility into, and understanding of, how the technology they acquire is developed,
516 integrated, and deployed, as well as the processes, procedures, and practices used to ensure the

---

[1] See definitions suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers in Appendix F, Glossary.
[2] NIST SP 800-53 Rev. 5 defines Information System as:

*An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial control systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.*

517   security, resilience, reliability, safety, integrity, and quality of the products and services.[3] Threats
518   and vulnerabilities created by malicious actors (individuals, enterprises, or nation states) are
519   often especially sophisticated and difficult to detect, and thus provide a significant risk to
520   enterprises. It should be noted that products (including software libraries, frameworks, toolkits,
521   Enterprise Resource Planning (ERP) solutions, and cloud-based resources) or services
522   originating both domestically or abroad might contain vulnerabilities that present opportunities
523   for cyber supply chain compromises.[4] For example, an adversary may have the power to insert
524   malicious capability into a product or to coerce a manufacturer to hand over the manufacturing
525   specifications of a sensitive U.S. system. Note that it is impossible to completely eliminate all
526   cyber supply chain risks.
527
528   Currently, enterprises and many private sector suppliers, developers, system integrators, external
529   system service providers, and other ICT/OT-related service providers use varied and not yet
530   sufficiently standardized practices, which make it difficult to consistently measure and manage
531   cyber supply chain risks across different enterprises.
532

533   In this document, the practices and controls described for Cyber Supply Chain Risk
534   Management (C-SCRM) apply to both information technology (IT) and OT environments.
535   Similar to IT environments relying on ICT products and services, OT environments rely on OT
536   and ICT products and services, which create a cyber risk from ICT/OT products, services,
537   suppliers and their supply chains. Organizations should include OT-related suppliers,
538   developers, system integrators, external system service providers, and other ICT/OT-related
539   service providers within the scope of their C-SCRM activities.

540
541   When engaging with suppliers, developers, system integrators, external system service providers,
542   and other ICT/OT-related service providers, agencies should carefully consider the breadth of the
543   Federal government's footprint and the high likelihood that individual agencies may enforce
544   varying and conflicting C-SCRM requirements. Overcoming this complexity requires
545   interagency coordination and partnerships. The passage of the Federal Acquisition Supply Chain
546   Security Act (FASCSA) of 2018 aimed to address this concern by creating a government-wide
547   approach to the problem of supply chain security in federal acquisitions by establishing the
548   Federal Acquisition Security Council (FASC). The FASC therefore serves as a focal point of
549   coordination and information sharing and a harmonized approach to acquisition security that
550   addresses C-SCRM in acquisition processes and procurements across the federal enterprise. In
551   addition, the law incorporated SCRM into FISMA by requiring reporting on progress and

---

[4] This document adapts the definition of risk from [FIPS 200] to establish a definition for cyber supply chain risk as follows:

   *Risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.*

[4] This document defines a Cyber Supply Chain Compromise as:

   *Cyber supply chain incident (also known as compromise) is an occurrence within the supply chain whereby the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits is jeopardized. A cyber supply chain incident can occur anywhere during the life cycle of the system, product or service.*

[5] Appendix F, Glossary

552 effectiveness of the agency's supply chain risk management consistent with guidance issued by
553 the Office of Management and Budget and the Council.
554
555 **1.1.    PURPOSE**
556
557 Cyber Supply Chain Risk Management (C-SCRM) is a systematic process for managing cyber
558 supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and
559 developing response strategies to the cyber supply chain risks presented by the supplier, the
560 supplied products and services, or the supply chain.[5] The purpose of this publication is to
561 provide guidance to organizations on how to identify, assess, select, and implement risk
562 management processes and mitigating controls across the organization to help manage cyber
563 supply chain risks.
564
565 The processes and controls identified in this document can be modified or augmented with
566 organization-specific requirements from policies, guidelines, response strategies, and other
567 sources. This publication empowers organizations to develop C-SCRM strategies that are
568 tailored to their specific mission/business needs, threats, and operational environments.
569
570 **1.2.    TARGET AUDIENCE**
571
572 C-SCRM is an organization-wide activity that should be directed under the overall enterprise
573 governance, regardless of the specific organizational structure.
574
575 This publication is intended to serve a diverse audience involved in C-SCRM, including:
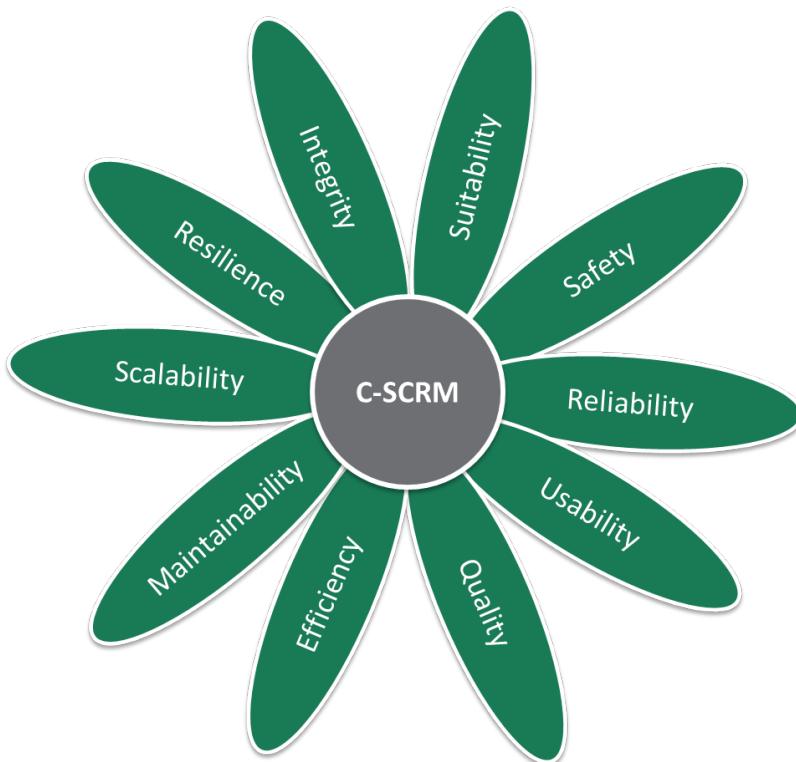
576 • Individuals with system, information security, privacy, or risk management and oversight
577   responsibilities, including authorizing officials (AOs), chief information officers, senior
578   information security officers, and senior officials for privacy;

579 • Individuals with system development responsibilities, including mission or business owners,
580   program managers, system engineers, system security engineers, privacy engineers, hardware
581   and software developers, system integrators, and acquisition or procurement officials;

582 • Individuals with acquisition and procurement-related responsibilities, including acquisition
583   officials and contracting officers;

584 • Individuals with logistical or disposition-related responsibilities, including program
585   managers, procurement officials, system integrators, and property managers;

586 • Individuals with security and privacy implementation and operations responsibilities,
587   including mission or business owners, system owners, information owners or stewards,
588   system administrators, continuity planners, and system security or privacy officers;

589 • Individuals with security and privacy assessment and monitoring responsibilities, including
590   auditors, Inspectors General, system evaluators, control assessors, independent verifiers and
591   validators, and analysts; and

592   • Commercial entities, including industry partners, that produce component products and
593     systems, create security and privacy technologies, or provide services or capabilities that
594     support information security or privacy.

595   **1.3.    BACKGROUND**

596

597   C-SCRM encompasses activities that span the entire system development life cycle (SDLC),
598   including research and development, design, manufacturing, acquisition, delivery, integration,
599   operations and maintenance, disposal, and overall management of an organization's products and
600   services. C-SCRM lies at the intersection of security, resilience, reliability, safety, integrity, and
601   quality, as depicted in Figure 1-1.

602



603
604                      **Fig. 1-1: Dimensions of C-SCRM**

605   • Security provides the confidentiality, integrity, and availability of information that (a)
606     describes the cyber supply chain (e.g., information about the paths of products and
607     services, both logical and physical) or (b) traverses the cyber supply chain (e.g.,
608     intellectual property contained in products and services), as well as information about the
609     parties participating in the cyber supply chain (anyone who touches a product or service
610     throughout its life cycle);
611   • Resilience is focused on ensuring the cyber supply chain will provide required products
612     and services and these products and services will be able to sufficiently perform or
613     recover, under stress or failure;

614 • Reliability is focused on the ability of a product or service to function as defined for a
615   specified period of time in a predictable manner;[6]
616 • Safety is focused on ensuring the product or service are free from conditions that can
617   cause death, injury, occupational illness, damage to or loss of equipment or property, or
618   damage to the environment;[7]
619 • Integrity is focused on ensuring the products or services in the cyber supply chain are
620   genuine, unaltered, and the products and services will perform according to acquirer
621   specifications and without additional unwanted functionality; and
622 • Quality is focused on meeting or exceeding performance, technical, and functional
623   specifications while ensuring vulnerabilities are mitigated that may limit the intended
624   function of a component or delivery of a service, lead to component or service failure, or
625   provide opportunities for exploitation.
626

627 **1.3.1. The Business Case for C-SCRM**

628

629 Today, every organization heavily relies on digital technology to fulfill its business and mission.
630 Digital technology is comprised of ICT/OT products and is delivered through and supported by
631 services. C-SCRM is a critical capability that every organization needs to have to address cyber
632 risks posed by the use of digital technology to support its business and mission. The depth,
633 extent, and maturity of a C-SCRM capability for each organization should be based on the
634 uniqueness of business or mission, organization-specific compliance requirements, operational
635 environment, risk appetite, and risk tolerance.
636

637 Establishing and sustaining a C-SCRM capability creates a number of significant benefits:
638

639 • Reduced likelihood of cyber supply chain compromise. Well-designed C-SCRM
640   processes and controls achieve this by enhancing an organization's ability to effectively
641   detect, respond, and recover from events that result in significant business disruptions,
642   should a C-SCRM compromise occur.
643 • Operational and organizational efficiencies achieved through clear structure, purpose, and
644   alignment of C-SCRM capabilities and prioritization, consolidation, and streamlining of
645   existing C-SCRM processes.
646 • Greater assurance that products acquired are of high quality, authentic, reliable, resilient,
647   maintainable, secure, and safe.
648

649 Greater assurance that service providers are trustworthy and can be relied upon to meet their
650 performance requirements. Organizations should carefully consider the potential costs of
651 applying C-SCRM processes and controls, weighing such costs against the risk to the
652 organization were they not applied. Implementing C-SCRM processes and controls will require
653 financial and human resources, as well as tools and infrastructure investments, not only from the
654 organizations themselves, but also from their suppliers, developers, system integrators, external
655 system service providers, and other ICT/OT-related service providers which may also result in
656 increased costs to the acquirer. Such costs may be realized through required staff upskilling or

---

[6] NIST SP 800-160 Vol.2
[7] NIST SP 800-160 Vol.2

657    hiring, vendor switching, impacts on contingency planning, supplier diversity, and procurement
658    timeline delays.
659
660    The passage of the 2018 SECURE Technology Act, formation of the Federal Acquisition
661    Security Council (FASC), and the observations from the 2015 and 2019 Case Studies in Cyber
662    Supply Chain Risk Management captured in the National Institute of Standards and Technology
663    Interagency Report (NISTIR) 8276, *Key Practices in Cyber Supply Chain Risk Management*,
664    point to broad public and private sector consensus: C-SCRM capabilities are a critical and
665    foundational component of any organization's risk posture.
666
667    ### 1.3.2.   Organization's Cyber Supply Chain
668
669    Today's organizations run complex information systems and networks to support their missions.
670    These information systems and networks are composed of ICT/OT[8] products and components
671    made available by *suppliers, developers, and system integrators*. Organizations also acquire and
672    deploy an array of services, that include but are not limited to:
673
674    - Building custom software for information systems that are to be deployed within the
675      organization, made available by *developers;*
676    - Integrating or providing operations, maintenance, and disposal support for information
677      systems and networks within and outside of the organization's boundaries,[9] made
678      available by *system integrators or other ICT/OT-related service providers;* and
679    - Providing external services to support organization's operations that are positioned both
680      inside or outside of the authorization boundaries, made available by *external system
681      service providers*.
682
683    These services may span the entire SDLC for an information system or service and may be:
684
685    - Performed by the staff employed by the organization, developer, system integrator, or
686      external system service provider;
687    - Be physically hosted by the organization or by the developer, system integrator, or
688      external system service provider;
689    - Supported or comprised of development environments, logistics/delivery environments
690      that transport information systems and components, or applicable system and
691      communications interfaces;
692    - Using Commercial-off-the-Shelf (COTS) hardware and software.
693

---

[8] NIST SP 800-37 Rev. 2 defines Operational Technology as:
   *Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical
   environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and
   events. Examples include industrial control systems, building management systems, fire control systems, and physical access control
   mechanisms.*

[9] For federal information systems, this is the Authorization Boundary, defined in NIST SP 800-53 Rev. 5 as:
   *All components of an information system to be authorized for operation by an authorizing official. This excludes
   separately authorized systems to which the information system is connected.*
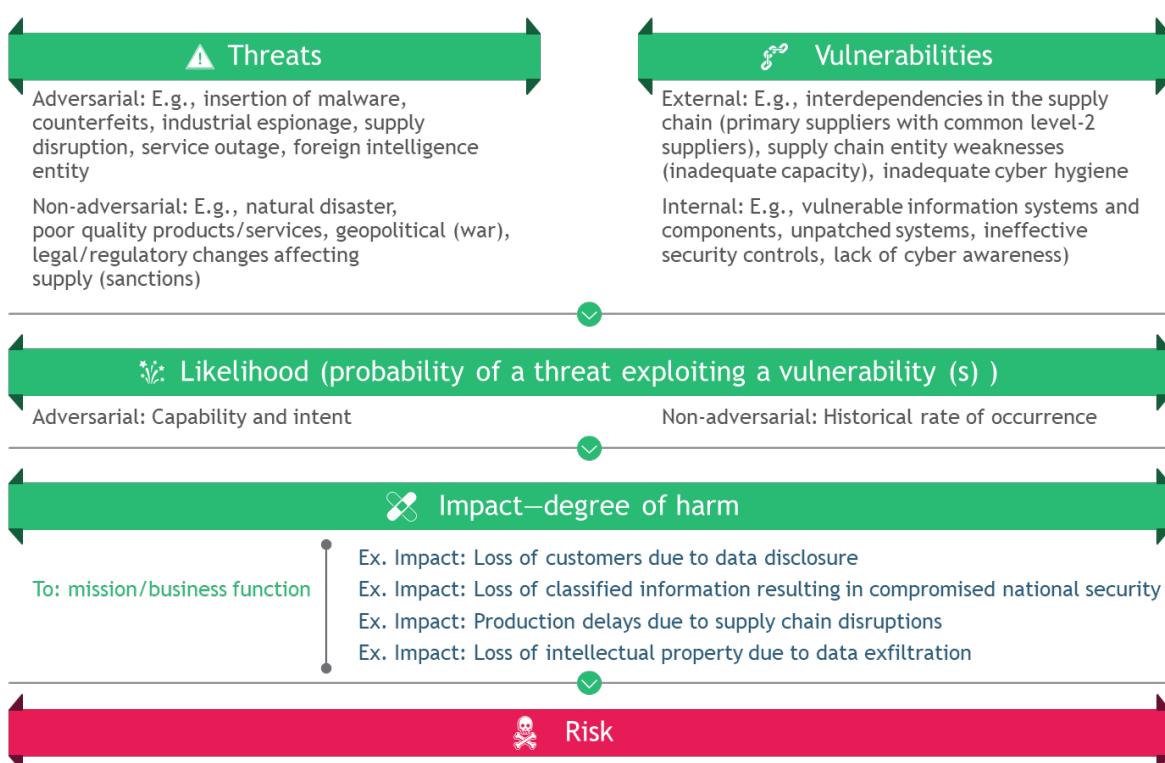
694    The responsibility and accountability for the services and associated activities performed by
695    different parties within this ecosystem are usually defined by agreement documents between the
696    organization and suppliers, developers, system integrators, external system service providers, and
697    other ICT/OT-related service providers.
698

699    **1.3.3.  Cyber Supply Chain Risk**
700

701    Cyber supply chain risks include, but are not limited to, the insertion of counterfeits,
702    unauthorized production, malicious insiders, tampering, theft, insertion of malicious software
703    and hardware (e.g., Global Positioning System (GPS) tracking devices, computer chips, etc.), as
704    well as poor manufacturing and development practices in the cyber supply chain. These risks are
705    realized when threats in the cyber supply chain exploit existing vulnerabilities.
706

707    Figure 1-2 depicts cyber supply chain risk resulting from the likelihood that relevant threats may
708    exploit applicable vulnerabilities and the consequential potential impact.
709

## Cyber Supply Chain Risk

| ⚠ Threats | 🔗 Vulnerabilities |
|---|---|
| Adversarial: E.g., insertion of malware, counterfeits, industrial espionage, supply disruption, service outage, foreign intelligence entity | External: E.g., interdependencies in the supply chain (primary suppliers with common level-2 suppliers), supply chain entity weaknesses (inadequate capacity), inadequate cyber hygiene |
| Non-adversarial: E.g., natural disaster, poor quality products/services, geopolitical (war), legal/regulatory changes affecting supply (sanctions) | Internal: E.g., vulnerable information systems and components, unpatched systems, ineffective security controls, lack of cyber awareness) |

**⚶ Likelihood (probability of a threat exploiting a vulnerability (s) )**

Adversarial: Capability and intent                    Non-adversarial: Historical rate of occurrence

**⚗ Impact—degree of harm**

To: mission/business function

Ex. Impact: Loss of customers due to data disclosure
Ex. Impact: Loss of classified information resulting in compromised national security
Ex. Impact: Production delays due to supply chain disruptions
Ex. Impact: Loss of intellectual property due to data exfiltration

**☠ Risk**

710

711                              **Fig. 1-2: Cyber Supply Chain Risk**
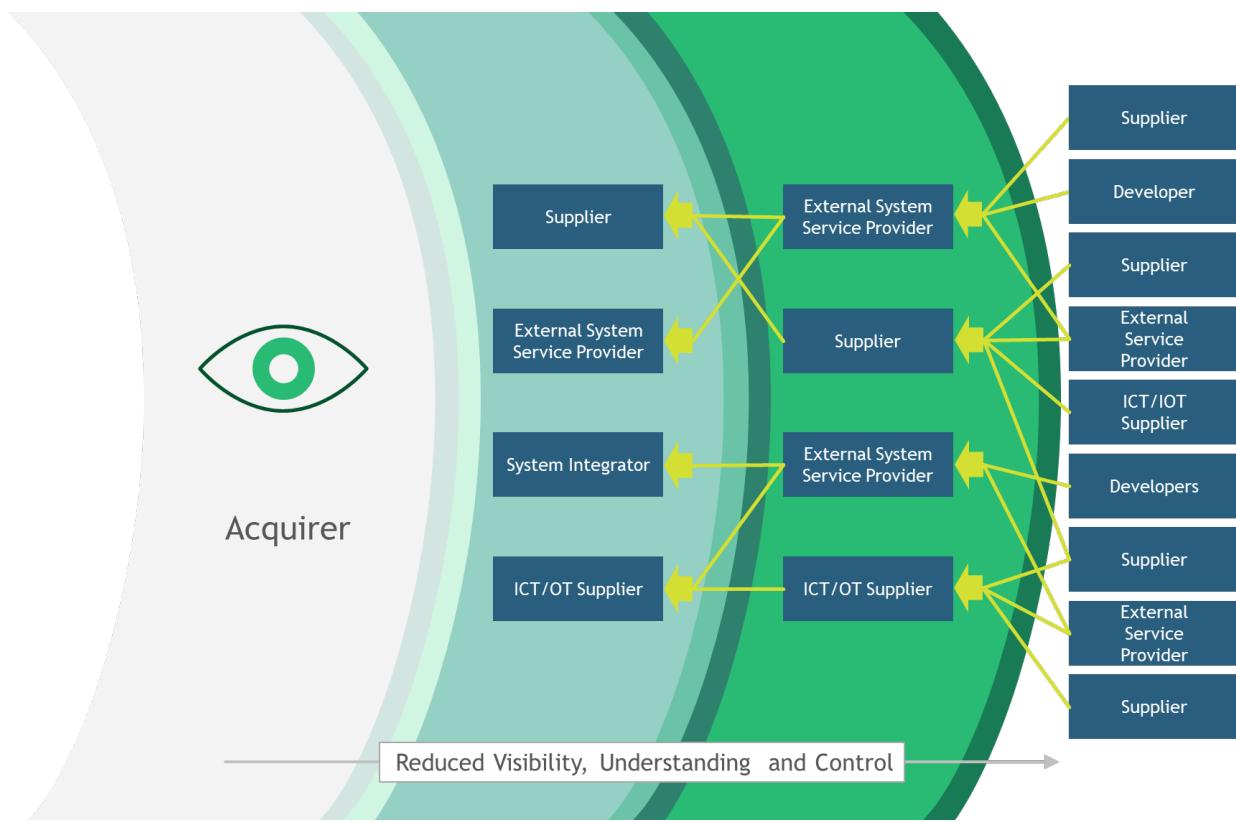
712    Cyber supply chain vulnerabilities may lead to a persistent negative impact on an organization's
713    missions ranging from reduction in service levels leading to customer dissatisfaction to theft of

714   intellectual property or degradation of critical mission and business processes.  However, it
715   might take years for such vulnerability to be exploited or discovered. It may also be difficult to
716   determine whether an event was the direct result of a supply chain vulnerability. Shared
717   vulnerabilities in the supply chain may also expose organizations to cascading cyber supply
718   chain risks. For example: a large-scale service outage at a major cloud services provider may
719   cause service or production disruptions for multiple entities within an organization's supply
720   chain and lead to negative effects within multiple mission and business processes.
721

722   **1.3.4.  Supplier Relationships within Organizations**
723

724   Cyber supply chain risks are associated with an organization's decreased visibility into, and
725   understanding of, how the technology they acquire is developed, integrated, and deployed and
726   how the services they acquire are delivered. They are also associated with the processes,
727   procedures, and practices used to ensure the security, safety, integrity, quality, reliability,
728   trustworthiness or authenticity of a product, service or source of the products and services.
729   Federal agencies have a variety of relationships with their suppliers, developers, system
730   integrators, external system service providers, and other ICT/OT-related service providers.
731   Figure 1-3 depicts how these diverse types of relationships affect an organization's visibility and
732   control of the supply chain.
733
734

735



736

**Fig. 1-3: An Organization's Visibility, Understanding, and Control of its Cyber Supply Chain**

Some supply chain relationships are tightly intermingled, such as the development by a system integrator of a complex information system designed to operate within the federal agency's authorization boundary, or the management of federal agency information systems and resources by an external service provider. These relationships are usually guided by an agreement (e.g., contract) that establishes detailed functional, technical, and security requirements and may provide for custom development or significant customization of products and services. For these relationships, system integrators and external service providers are likely able to work with the organization to implement such processes and controls (listed within this document) which are deemed appropriate based on the results of a criticality and risk assessment and cost/benefit analysis. This may include floating requirements upstream in the supply chain to ensure higher confidence in the satisfaction of necessary assurance objectives. The decision to extend such requirements must be balanced with an appreciation of what is feasible and cost-effective. The degree to which system integrators and external service providers are expected to implement C-SCRM processes and controls should be weighed against the risks to the organization posed by not adhering to those additional requirements. Often, working directly with the system integrators and external service providers to proactively identify appropriate mitigation processes and controls will help create a more cost-effective strategy.

757   Procuring ICT/OT products directly from suppliers establishes a direct relationship between
758   those suppliers and the acquirers. This relationship is also usually guided by an agreement
759   between the acquirer and the supplier. However, commercial ICT/OT developed by suppliers are
760   typically designed for general purposes for a global market and are not typically tailored to an
761   individual customer's specific operational or threat environments. Organizations should perform
762   due diligence research regarding their specific C-SCRM requirements to determine if an IT
763   solution is "fit for purpose[10]," includes requisite security features and capabilities, will meet
764   quality and resiliency expectations, and if and how the supplier will provide support for the
765   product, or product components, over its life cycle.
766
767   An assessment of the findings of an acquirer's research about a product—which may include
768   engaging in a dialog directly with suppliers whenever possible—will help acquirers understand
769   the characteristics and capabilities of existing ICT/OT products and services, set expectations
770   and requirements for suppliers, and identify C-SCRM needs not yet satisfied by the market. It
771   can also help identify emerging solutions that may at least partially support the acquirer's needs.
772   Overall, such research and engagement with a supplier will allow the acquirer to better articulate
773   their requirements to align with and drive market offerings and make risk-based decisions about
774   product purchases, configurations, and usages within their environment.
775

---

**Managing Cost and Resources**

776

778   Balancing cyber supply chain risks with the costs and benefits of C-SCRM controls should be a
779   key component of the acquirer's overall approach to C-SCRM.
780
781   Organizations should be aware that implementing C-SCRM controls necessitates additional
782   financial and human resources. Requiring a greater level of testing, documentation, or security
783   features from suppliers, developers, system integrators, external system service providers, and
784   other ICT/OT-related service providers may increase the price of a product or service which may
785   result in increased cost to the acquirer. This is especially true for those products and services
786   developed for general-purpose application and not tailored to the specific organization's security
787   or C-SCRM requirements. In the decision whether to require and implement C-SCRM controls,
788   acquirers should consider both the costs of implementing these controls and the risks of not
789   implementing them.
790

---

791
792   To mitigate the costs and when appropriate, acquirers should allow suppliers, developers, system
793   integrators, external system service providers, and other ICT/OT-related service providers the
794   opportunity to reuse any existing data and documentation that may provide evidence to support
795   C-SCRM.
796
797

---

[10] "Fit for purpose" is a term used informally to describe a process, configuration item, IT service, etc., that is capable of meeting its objectives or service levels. Being fit for purpose requires suitable design, implementation, control, and maintenance. (Adapted from Information Technology Infrastructure Library (ITIL) Service Strategy [ITIL Service Strategy].)

## 1.4.  C-SCRM KEY PRACTICES

Cyber supply chain risk management builds on existing standardized practices in multiple disciplines, as well as the evolution of C-SCRM capabilities. Organizations should prioritize reaching a base level of maturity in key practices prior to specifically focusing on advanced C-SCRM capabilities. Those key practices are described in NIST standards and guidelines, such as NISTIR 8276, as well as other applicable national and international standards and best practices. They include: integrating C-SCRM across the organization; establishing a formal program; knowing and managing critical products, services, and suppliers; understanding an organization's supply chain; closely collaborating with key suppliers; including key suppliers in resilience and improvement activities; assessing and monitoring throughout the supplier relationship; and, planning for the full lifecycle.

### 1.4.1.  Foundational Practices

Having foundational practices in place is critical to successfully and productively interacting with system integrators and suppliers may be at varying levels themselves regarding having such practices standardized and in place. The following are specific examples of the recommended multidisciplinary foundational practices that can be implemented incrementally to improve an organization's ability to develop and execute more advanced C-SCRM practices:

- Establish a core, dedicated multi-disciplinary C-SCRM Program Management Office and/or C-SCRM team;
- Implement a risk management hierarchy and risk management process (in accordance with NIST SP 800-39, *Managing Information Security Risk* [NIST SP 800-39]) including an organization-wide risk assessment process (in accordance with NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [NIST SP 800-30 Rev. 1]);
- Establish an organization governance structure that integrates C-SCRM requirements and incorporates these requirements into the organizational policies;
- Develop a process for identifying and measuring the criticality of the organization's suppliers, products and services;
- Raise awareness and foster understanding of what C-SCRM is and why it is critically important;
- Develop and/or integrate C-SCRM into acquisition/procurement policies and procedures (including Federal Information Technology Acquisition Reform Act (FITARA) processes, applicable to federal agencies) and purchase card processes;
- Establish consistent, well-documented, repeatable processes for determining [Federal Information Processing Standards (FIPS) 199] impact levels;
- Establish and begin using supplier risk assessment processes on a prioritized basis (inclusive of criticality analysis, threat analysis, and vulnerability analysis) after the [FIPS 199] impact level has been defined;
- Implement a quality and reliability program that includes quality assurance and quality control process and practices;
- Establish explicit collaborative and discipline-specific roles, accountabilities, structures, and processes for supply chain, cybersecurity, product security, and physical security

11

843     (and other relevant) processes (e.g., Legal, Risk Executive, Human Resources (HR),
844     Finance, Enterprise IT, Program Management/System Engineering, Information Security,
845     Acquisition/procurement, supply chain logistics, etc.);
846 • Ensure that adequate resources are dedicated and allocated to information security and C-
847     SCRM to ensure proper implementation of policy, guidance, and controls;
848 • Ensure there are sufficiently cleared personnel, with key C-SCRM roles and
849     responsibilities, to access and share C-SCRM-related classified information.
850 • Implement an appropriate and tailored set of baseline information security controls found
851     in NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems
852     and Organizations [NIST SP 800-53 Rev. 5];
853 • Establish internal checks and balances to ensure compliance with security and quality
854     requirements;
855 • Establish a supplier management program including, for example, guidelines for
856     purchasing directly from qualified original equipment manufacturers (OEMs)[11] or their
857     authorized distributors and resellers; and
858 • Implement a robust incident management program to successfully identify, respond to,
859     and mitigate security incidents. This program should be capable of identifying causes of
860     security incidents, including those originating from the cyber supply chain.
861

### 1.4.2. Sustaining Practices

862

863

864 Sustaining practices should be used to enhance the efficacy of cyber supply chain risk
865 management. These practices are inclusive of and build upon foundational practices.
866 Organizations that have standardized and implemented the foundational practices broadly should
867 consider these practices as next steps in advancing their cyber supply chain risk management
868 capabilities:
869

870 • Use third-party assessments, site visits, and formal certification to assess critical
871     suppliers;
872 • Use the organization's understanding of its C-SCRM risk profile (or risk profiles, specific
873     to mission/business areas) to define a risk appetite and risk tolerances to empower leaders
874     with delegated authority across the organization to make C-SCRM decisions in alignment
875     with organization's mission imperatives and its strategic goals and objectives;
876 • Use a formalized information sharing function to engage with the FASC as well as other
877     government agencies to enhance the organization's cyber supply chain threat and risk
878     insights and help ensure a coordinated and holistic government-wide approach to
879     addressing cyber-supply chain risks that may affect a broader set of agencies or national
880     security;
881 • Embed C-SCRM specific training into training curriculums of applicable roles across the
882     organization processes involved with C-SCRM including but not limited to information
883     security, procurement, risk management, engineering, software development, IT, legal,
884     and HR;

---

[11] For purposes of this publication, the term *original equipment manufacturers* includes *original component manufacturers*.

885 • Integrate C-SCRM considerations into every aspect of the system and product lifecycle,
886   implementing consistent, well-documented, repeatable processes for system engineering,
887   cybersecurity practices, and acquisition;
888 • Integrate the organization's defined C-SCRM requirements into contractual language
889   found in agreements with suppliers, developers, system integrators, external system
890   service providers, and other ICT/OT-related service providers;
891 • Include key suppliers in contingency planning, incident response, and disaster recovery
892   planning and testing;
893 • Engage with suppliers, developers, system integrators, external system service providers,
894   and other ICT/OT-related service providers to improve their cybersecurity practices; and
895 • Define, collect and report C-SCRM metrics to ensure cyber supply chain risk aware
896   leadership, enable active management of the completeness of C-SCRM implementations,
897   and drive efficacy of the organization's C-SCRM processes and practices.
898

## 899    1.4.3.  Enhancing Practices

900

901 Enhancing practices should be applied by the organization with the goal of advancement toward
902 adaptive and predictive C-SCRM capabilities. Organizations should pursue these practices once
903 sustaining practices have been broadly implemented and standardized across the organization:
904 • Automate C-SCRM processes where applicable and practical to drive execution
905   consistency, efficiency, and free up key resources to focus on other critical C-SCRM
906   activities;
907 • Adopt quantitative risk analyses that apply probabilistic approaches (e.g. Bayesian
908   Analysis, Monte Carlo Methods) to reduce uncertainty about cyber supply chain risk,
909   enhance organization leadership's ability to identify optimal risk responses, and measure
910   response effectiveness; and
911 • Apply insights gained from leading C-SCRM metrics (i.e., forward-looking indicators) to
912   shift from reactive to predictive C-SCRM strategies and plans that adapt to cyber supply
913   chain risk profile changes before they occur.

914 The guidance and controls contained in this publication are built on existing multidisciplinary
915 practices and are intended to increase the ability of organizations to strategically manage cyber
916 supply chain risks over the entire life cycle of systems, products, and services. Refer to Table 3-3
917 in Section 3 for a summary view of C-SCRM key practices.
918

## 919    1.5.    RELATIONSHIP TO OTHER PROGRAMS AND PUBLICATIONS

920

921 The revision to NIST SP 800-161 builds upon concepts described in a number of NIST and other
922 publications to facilitate integration with the agencies' existing organization-wide activities, as
923 well as a series of legislative developments following its initial release. These resources are
924 complementary and help organizations build risk-based information security programs to protect
925 their operations and assets against a range of diverse and increasingly sophisticated threats. This
926 publication will be revised to remain consistent with the NIST SP 800-53 security controls
927 catalog, using an iterative process as the C-SCRM discipline continues to mature.
928

929  **1.5.1.  NIST Publications**
930
931  NIST SP 800-161 Rev. 1 leverages the latest versions of the publications and programs that
932  guided its initial development, as well as new publications following its initial release:
933

934  •  NIST Cybersecurity Framework (CSF) Version 1.1;
935  •  FIPS 199, *Standards for Security Categorization of Federal Information and Information*
936  *Systems,* to conduct criticality analysis to scoping C-SCRM activities to high-impact
937  components or systems [FIPS 199];
938  •  NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments,* to integrate
939  ICT/OT SCRM into the risk assessment process [NIST SP 800-30 Rev. 1];
940  •  NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and*
941  *Organizations: A System Life Cycle Approach for Security and Privacy* [NIST SP 800-37
942  Rev. 2]*;*
943  •  NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and*
944  *Information System View,* to integrate ICT/OT SCRM into the risk management levels
945  and risk management process [NIST SP 800-39];
946  •  NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and*
947  *Organizations,* to provide information security controls for enhancing and tailoring to C-
948  SCRM context [NIST SP 800-53 Rev. 5];
949  •  NIST SP 800-53B Revision 5, *Control Baselines for Information Systems and*
950  *Organizations*, to codify control baselines and C-SCRM supplementary guidance and
951  [NIST SP 800-53B Rev. 5];
952  •  NIST SP 800-160 Vol. 1, *Systems Security Engineering* [NIST SP 800-160 Vol. 1] and
953  NIST SP 800-160 Vol. 2, *Developing Cyber Resilient Systems: A Systems Security*
954  *Engineering Approach* [NIST SP 800-160 Vol. 2] for specific guidance on the security
955  engineering aspects of C-SCRM;
956  •  NIST SP 800-181 Revision 1, *National Initiative for Cybersecurity Education (NICE)*
957  *Cybersecurity Workforce Framework*, as a means of forming a common lexicon on C-
958  SCRM workforce topics [NIST SP-800-181 Rev. 1];
959  •  NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal*
960  *Information Systems*, for background materials in support of applying the special
961  publication to their specific acquisition processes [NISTIR 7622];
962  •  NISTIR 8179, *Criticality Analysis Process Model: Prioritizing Systems and Components*,
963  to guide ratings of supplier criticality [NISTIR 8179];
964  •  NISTIR 8272, *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks* for
965  guidance on how to prioritize supplier criticality [NISTIR 8272];
966  •  NISTIR 8276, *Key Practices in Cyber Supply Chain Risk Management: Observations*
967  *from Industry*, to elucidate recent C-SCRM trends in the private sector [NISTIR 8276];
968  and
969  •  NISTIR 8286, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk*
970  *Management (ERM)*, to inform the content on integrating C-SCRM into enterprise risk
971  management [NISTIR 8286].
972

### 1.5.2. Regulatory and Legislative Guidance

NIST SP 800-161 Rev. 1 is informed heavily by the regulatory and legislative guidance, including:

- Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*; and
- The Federal Acquisition Supply Chain Security Act (FASCA), *Title II of the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology Act of 2018*.

### 1.5.3. Other U.S. Government Reports

NIST SP 800-161 Rev. 1 is also informed by a number of additional government reports:

- Government Accountability Office (GAO) Report, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks*, December 2020, GAO-21-171 [GAO]
- Department of Defense and Department of Homeland Security Software Assurance Acquisition Working Group, *Software Assurance in Acquisition: Mitigating Risks to the Enterprise* [SwA];
- National Defense Industrial Association (NDIA), *Engineering for System Assurance* [NDIA];

### 1.5.4. Standards, Guidelines, and Best Practices

Additionally, NIST SP 800-161 draws its inspiration from a number of international standards, guidelines, and best practice documents:

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 15288 – *Systems and software engineering – System Life Cycle Processes* [ISO/IEC 15288];
- ISO/IEC 27036 – *Information Technology – Security Techniques – Information Security for Supplier Relationships* [ISO/IEC 27036];
- ISO/IEC 20243 – *Information Technology — Open Trusted Technology Provider^TM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products* [ISO/IEC 20243];
- ISO/IEC 27000 – *Information Technology – Security Techniques – Information Security Management System – Overview and Vocabulary* [ISO/IEC 27000];
- ISO/IEC 27002 – *Information Technology – Security Techniques – Code of Practice for Information Security Controls* [ISO/IEC 27002];
- Software Assurance Forum for Excellence in Code (SAFECode) *Software Integrity Framework* [SAFECode 2] and *Software Integrity Best Practices* [SAFECode 1]; and
- Cyber Risk Institute, *Financial Services Cybersecurity Framework Profile Version 1.1* [FSP].

### 1.5.5. Guidance for Cloud Service Providers

The *external system service providers* discussed in this publication include *cloud service providers*. This publication does not replace guidance provided with respect to federal agency

1017  assessment of cloud service providers' security.  When applying this publication to cloud service
1018  providers, federal agencies should first use Federal Risk and Authorization Program (FedRAMP)
1019  cloud services security guidelines and then apply NIST SP 800-161 Rev. 1 for those processes
1020  and controls that are not addressed by FedRAMP. [12]
1021
1022  **1.6.    METHODOLOGY FOR BUILDING C-SCRM GUIDANCE USING SP 800-39, SP**
1023  **        800-37 REVISION 2, AND NIST SP 800-53 REVISION 5**
1024
1025  This publication applies the multileveled risk management approach of [NIST SP 800-39], by
1026  providing C-SCRM guidance at organization, mission, and operational-levels. It also introduces
1027  a navigational system for SP 800-37 Rev. 2, allowing users to more easily focus on relevant
1028  sections of this publication. Finally, it contains an enhanced overlay of specific C-SCRM
1029  controls, building on NIST SP 800-53 Revision 5.
1030
1031  The guidance/controls contained in this publication are built on existing multidisciplinary
1032  practices and are intended to increase the ability of organizations to strategically and
1033  operationally manage the associated cyber supply chain risks over the entire life cycle of
1034  systems, products, and services. It should be noted that this publication gives organizations the
1035  flexibility to either develop stand-alone documentation (e.g., policies, assessment and
1036  authorization [A&A] plan and C-SCRM plan) for C-SCRM or to integrate it into existing agency
1037  documentation.
1038
1039  For individual systems, this guidance is recommended for use with information systems at all
1040  impact categories, according to [FIPS 199]. The agencies may choose to prioritize applying this
1041  guidance to systems at a higher-impact level or to specific system components. Finally, NIST SP
1042  800-161 Rev. 1 describes the development and implementation of C-SCRM Strategies and
1043  Implementation Plans for development at the enterprise and mission/business level of an
1044  organization and a C-SCRM system plan at the operational level of an organization. A C-SCRM
1045  plan at the operational level is informed by the cyber supply chain risk assessment and should
1046  contain C-SCRM controls tailored to specific agency mission/business needs, operational
1047  environments, and/or implementing technologies.
1048
1049  **1.6.1.  Integration into Risk Management Process**
1050
1051  The processes in this publication should be integrated into agencies' existing SDLCs and
1052  organizational environments at all levels of risk management processes and hierarchy
1053  (organization, mission, system) as described in [NIST SP 800-39]. Section 2 provides an
1054  overview of the [NIST SP 800-39] risk management hierarchy and approach and identifies C-
1055  SCRM activities in the risk management process. Appendix C builds on Section 2 of [NIST SP
1056  800-39], providing descriptions and explanations of ICT/OT SCRM activities. The structure of
1057  Appendix C mirrors [NIST SP 800-39].
1058

---

[12] For cloud services, FedRAMP is applicable for low-, moderate-, high-impact systems [FedRAMP]. Ongoing work will address
high-impact systems utilizing cloud services. Once the work is completed, agencies should refer to FedRAMP for guidance
applicable to high-impact systems utilizing cloud services.

1059   *1.6.2.*   **Implementing C-SCRM in the Context of SP 800-37 Revision 2**
1060
1061   C-SCRM activities described in this publication are closely related to the Risk Management
1062   Framework described in [NIST SP 800-37, Rev. 2]. Specifically, C-SCRM processes conducted
1063   at the operational level should closely mirror and/or serve as inputs to those steps completed as
1064   part of the [NIST SP 800-37, Rev 2]. C-SCRM activities completed at Levels 1 and 2 should
1065   provide inputs (e.g., risk assessment results) to the operational-level, RMF-type processes where
1066   possible and applicable. Section 2 and Appendix C describe in further detail the linkages
1067   between C-SCRM and [NIST SP 800-37, Rev. 2].
1068
1069   **1.6.3.   Enhanced C-SCRM Overlay**
1070
1071   This publication contains an enhanced overlay of [NIST SP 800-53 Rev. 5]. Appendix A
1072   identifies, refines, and expands C-SCRM-related controls from [NIST SP 800-53 Rev. 5], adds
1073   new controls that address specific C-SCRM concerns, and offers C-SCRM-specific supplemental
1074   guidance where appropriate. Figure 1-4 illustrates the process used to create the enhanced
1075   overlay. The individual controls and enhancements from [NIST SP 800-53 Rev. 5] that were
1076   relevant to C-SCRM were extracted. These controls were analyzed to determine how they apply
1077   to C-SCRM. Additional supplemental guidance was then developed and included for each
1078   control and control enhancement. The resulting set of controls and enhancements were evaluated
1079   to determine whether all C-SCRM concerns were addressed.
1080
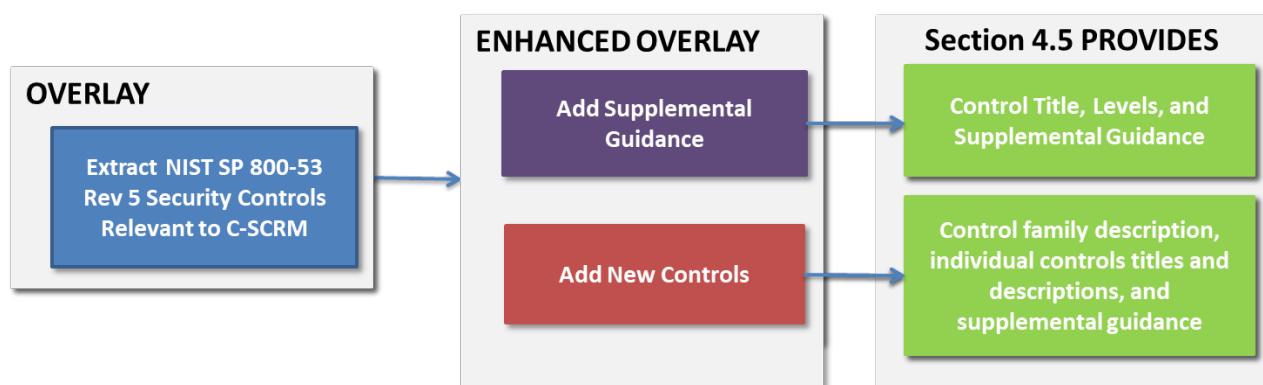
1081
1082
1083
1084          **Fig. 1-4: C-SCRM Security Controls in NIST SP 800-161, Revision 1, Section 4.5**

1085
1086   **1.7.      ORGANIZATION OF THIS SPECIAL PUBLICATION**
1087
1088   This publication is organized as follows:
1089   •   Section 1 provides the purpose, scope, and applicability of the publication and describes
1090       foundational concepts and practices;
1091   •   Section 2 discusses C-SCRM processes and how to integrate them into the organizational
1092       risk management hierarchy and risk management process, based on NIST SP 800-39;
1093   •   Section 3 discusses critical success factors for C-SCRM;
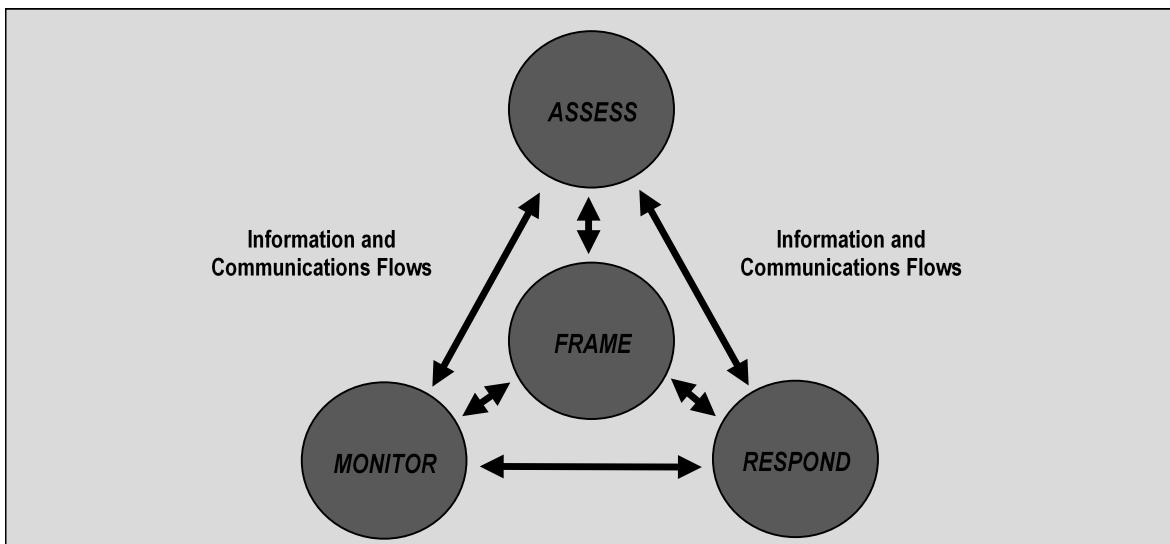
1094        • Section 4 contains implementation guidance for C-SCRM controls;

1095        • Appendix A provides C-SCRM controls summary;

1096        • Appendix B provides a set of example cyber supply chain risk exposure scenarios;

1097        • Appendix C provides C-SCRM activities in the Risk Management Process;

1098        • Appendix D provides a set of C-SCRM templates to include C-SCRM Strategy and
1099           Implementation Plan, C-SCRM Policy, C-SCRM Plan and C-SCRM Risk Assessment;

1100        • Appendix E provides a glossary of terms used in the publication;

1101        • Appendix F provides the acronyms and abbreviations used in the publication;

1102        • Appendix G lists references used in the development of this publication.

1103

1104

1105 **2. INTEGRATION OF C-SCRM INTO ENTERPRISE-WIDE RISK MANAGEMENT**

1106
1107 C-SCRM should be integrated into the enterprise-wide risk management process described in
1108 [NIST SP 800-39] and depicted in Figure 2-1. This process includes the following continuous
1109 and iterative steps:
1110    (i) Frame risk. Establish the context for risk-based decisions and the current state of the
1111        organization's information and communications technology and services, and the
1112        associated supply chain;
1113    (ii) Assess risk. Review and interpret criticality, threat, vulnerability, likelihood, impact, and
1114        related information;
1115    (iii)Respond. Select, tailor, and implement mitigation controls based upon risk assessment
1116        findings; and
1117    (iv)Monitor risk exposure and effectiveness in mitigating risk, on an ongoing basis, including
1118        tracking changes to an information system or supply chain, using effective organizational
1119        communications and a feedback loop for continuous improvement.
1120



1121
1122                              **Fig. 2-1: Risk Management Process**

1123
1124 Managing cyber supply chain risks is a complex undertaking that requires a coordinated,
1125 interdisciplinary approach across an organization. Effective cyber supply chain risk management
1126 (C-SCRM) requires engagement from stakeholders inside the organization (e.g., departments,
1127 processes) as well as outside the organization (e.g., suppliers, developers, system integrators,
1128 external system service providers, and other ICT/OT-related service providers) to actively
1129 collaborate, communicate, and take actions to secure favorable C-SCRM outcomes.
1130 Organizations should aim to infuse perspectives from multiple disciplines and processes (e.g.,
1131 information security, procurement, enterprise risk management, engineering, software
1132 development, IT, legal, HR, etc.) into their approaches to managing cyber supply chain risk.
1133 Organizations may define explicit roles to bridge and integrate these processes as a part of an
1134 organization's broader risk management activities. This orchestrated approach is an integral part
1135 of an organization's effort to identify C-SCRM priorities, develop solutions, and incorporate C-

1136    SCRM into overall risk management decisions. Organizations should perform C-SCRM
1137    activities as a part of acquisition, SDLC, and broader organizational risk management processes.
1138    Embedded C-SCRM activities involve identifying and assessing applicable risks, determining
1139    appropriate mitigating actions, documenting selected risk response actions, and monitoring
1140    performance of C-SCRM activities. As exposure to supply chain risk differs across
1141    organizations, enterprise and mission-specific strategies and policies should set the tone and
1142    direction for C-SCRM across the organization.
1143

> Organizations should ensure that tailored C-SCRM plans are designed to:
> - Manage, rather than eliminate risk;
> - Ensure that operations are able to adapt to constantly emerging or evolving threats;
> - Be responsive to changes within their own organization, programs, and the supporting information systems; and
> - Adjust to the rapidly evolving practices of the private sector's global ICT supply chain.

1144
1145
1146    Section 2.1 describes the three-level risk management approach in terms of C-SCRM. Generally,
1147    senior leaders provide the strategic direction, mid-level leaders plan and manage programs and
1148    projects, and individuals on the front lines procure, develop, implement, and operate the products
1149    and perform the services in their supply chain. As part of a multifaceted approach, organizations
1150    may rely on a centralized, interdisciplinary team or program management office (PMO) to lead,
1151    perform, and coordinate Level 1 and Level 2 C-SCRM processes that inform C-SCRM processes
1152    at the Level 3 operational-level. Specific discussion of the full scope of C-SCRM PMO
1153    implementations and responsibilities is discussed later in this section. In general, the activities
1154    performed in each level can be integrated into an organization's overall risk management process
1155    in order to ensure that the C-SCRM program appropriately supports the organization's mission
1156    and goals.[13] Section 2.2 describes the Risk Management Framework as it applies to C-SCRM.
1157    The foundational concepts are described in greater detail in [NIST SP 800-39].
1158

---

[13] This document uses the word "mission" to mean the organization's required tasks as determined by the organization's purpose and enterprise-level goals and priorities.

**Fig. 2-2: Risk Appetite & Risk Tolerance**

Risk Appetite and Risk Tolerance play a critical role in enabling organizations to effectively manage exposure to cyber supply chain risks:
- Risk appetite represents the types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value [NISTIR 8286];
- Risk tolerance is the acceptable level of variation relative to achievement of a specific value objective;
- Risk appetite provides the management's expected bounds for taking risks in pursuit of value while risk tolerance provides the bounds not be exceeded;
- Refer to the appendix for further discussion on Risk Appetite & Risk Tolerance.

## 2.1. Multi-Level Risk Management

To integrate risk management throughout an organization, [NIST SP 800-39] describes three levels, depicted in Figure 2-2, that address risk from different perspectives: (i) enterprise-level; (ii) mission/business process level; and (iii) operational level. C-SCRM requires the involvement of all three levels.

**STRATEGIC RISK**

- Traceability and Transparency of Risk-Based Decisions

- Organization-Wide Risk Awareness

LEVEL 1
ENTERPRISE

LEVEL 2
MISSION / BUSINESS PROCESSES

LEVEL 3
OPERATIONAL

- Inter-Level and Intra-Level Communications
- Feedback Loop for Continuous Improvement

**TACTICAL RISK**
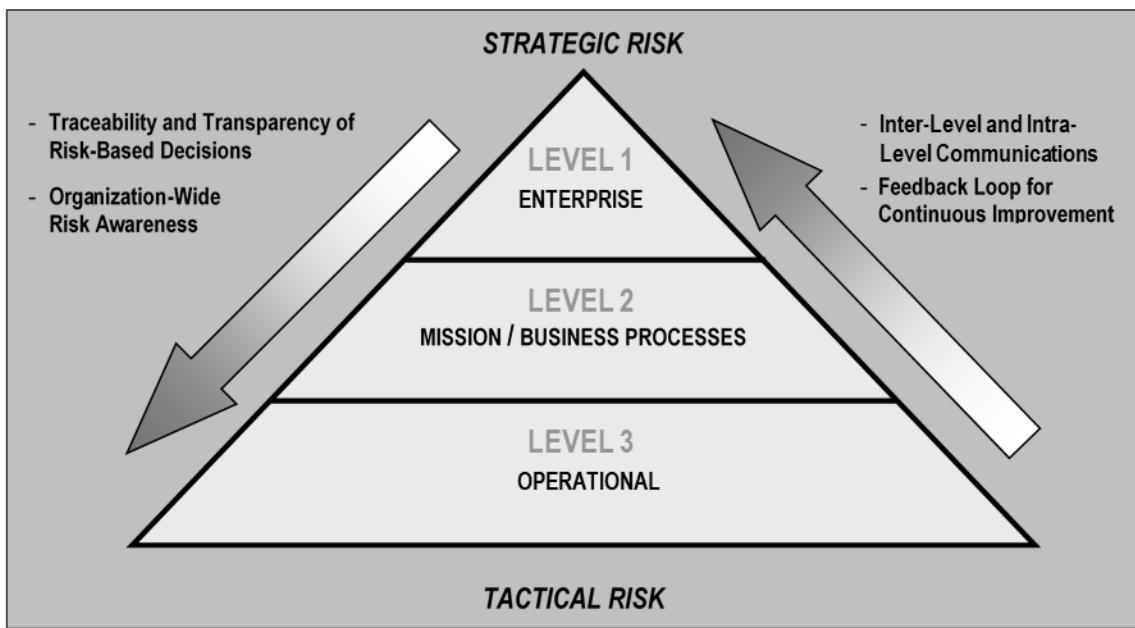
1171
1172     **Fig. 2-3: Multileveled Organization-wide Risk Management[14]**

1173
1174     In general, Level 1 is engaged in the organization-wide risk framing, the development of the
1175     overall C-SCRM strategy, the formation of interdisciplinary groups to engage on C-SCRM, the
1176     creation of the organization-wide policies, and a high-level implementation plan to guide C-
1177     SCRM activities performed at the mission and business process levels. Level 2 is engaged in
1178     developing mission-specific strategies that contextualize the enterprise-level strategy to the
1179     specific mission and business processes. Level 2 is also responsible for developing C-SCRM
1180     implementation plans that guide strategy implementation within the mission and business
1181     processes. C-SCRM activities performed at Level 2 include prioritizing the organization's
1182     mission and business processes, and conducting mission/business-level risk assessments,
1183     including supply chain risk assessments performed when procuring a product or service. Level 3
1184     is engaged in development of the C-SCRM Plans which guide the application of C-SCRM to
1185     specific information systems and information technology acquisitions, including its integration
1186     into SDLC processes that guide system development, operation, and maintenance activities.
1187     Across the organization, C-SCRM stakeholders coordinate with the various mission and business
1188     processes and information system teams to infuse C-SCRM and establish an overarching
1189     organizational capability to manage cyber supply chain risks.
1190

---

[14] Further information about the concepts depicted in Figure 2-2 can be found in [NIST SP 800-39].

Cyber supply chain risk ownership and accountability ultimately lies with the head of the organization:
- The organization's risk profile, risk appetite, and risk tolerance levels will inform who makes risk decisions and processes should address when and how escalation of risk decisions need to occur.
- Ownership should be delegated to authorizing officials within the agency based on their executive authority over organizational missions, business operations or information systems.
- Authorizing officials may further delegate responsibilities to designated officials who are responsible for the day-to-day management of risk.

1191
1192
1193 The C-SCRM activities can be performed by a variety of individuals or groups within an
1194 organization ranging from a single individual to committees, divisions, centralized program
1195 offices, or any other organizational structures. C-SCRM activities will be distinct for different
1196 organizations depending on their organization's structure, culture, mission, and many other
1197 factors.
1198
1199 For individual systems, the C-SCRM Plans provide the basis for determining whether an
1200 information system meets business, functional, and technical requirements and includes
1201 appropriately tailored controls. For missions and business processes, the C-SCRM Strategy and
1202 Implementation Plan provides specific C-SCRM activities that lay the foundation for an effective
1203 SCRM program and support the achievement of the organization's C-SCRM goals and
1204 objectives.  The C-SCRM Strategy provides direction and guidance at the enterprise level and
1205 should address the integration of C-SCRM considerations into the overall enterprise risk
1206 management strategy.  C-SCRM Strategy and Implementation Plan(s), and operational-level C-
1207 SCRM Plans help organizations focus appropriate resources on the most critical processes and
1208 components based on organizational mission/business requirements and their risk environment.
1209 Figure 2-3 depicts applicability of different types of C-SCRM documentation to the three risk
1210 management framework levels.
1211
1212 These plans are intended to be referenced regularly and should be reviewed and refreshed
1213 periodically.  These are not intended to be documents developed to satisfy a compliance
1214 requirement.  Rather, organizations should be able to demonstrate how they have historically and
1215 continue to effectively employ their plans to shape, align, inform, and take C-SCRM actions and
1216 decisions across all three levels.
1217

1218



**Fig. 2-4: C-SCRM Documents in Multi-Level Organization-wide Risk Management**

## 2.1.1.  Roles and Responsibilities Across the Three Levels

Implementing C-SCRM requires that organizations establish a coordinated team-based approach
to assess cyber supply chain risk and manage this risk by establishing and adhering to policies,
developing and following processes (often cross-organizational in nature), as well as employing
programmatic and technical mitigation techniques. The coordinated team approach, either ad hoc
or formal, enables organizations to more effectively conduct a comprehensive, multi-perspective,
analysis of their supply chain and to respond to risks, communicate with external
partners/stakeholders, and gain broad consensus regarding appropriate resources for C-SCRM.
This team works together to make decisions and take actions that require the input and
involvement of multiple perspectives and expertise and leverages, but does not replace those C-
SCRM responsibilities and processes that can and should be specifically assigned to an
individual organization or disciplinary area.  Examples of C-SCRM activities that require a team
approach include but are not limited to: developing a strategic sourcing strategy; incorporating
C-SCRM requirements into a solicitation; and determining options about how best to mitigate an
identified supply chain risk, especially one assessed to be significant.

Members of the C-SCRM team should be a diverse group of people involved in the various
aspects of the organization's key processes including but not limited to information security,
procurement, enterprise risk management,  engineering, software development,  IT, legal, and
HR.  Collectively, to aid in C-SCRM, these individuals should have an awareness of, and
provide expertise in, organizational processes and practices specific to their discipline area,
vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects

1245 and inter-dependencies of systems or information flowing through systems. The C-SCRM team
1246 may be an extension of an organization's existing information system risk management, include
1247 parts of a general risk management team, or operate out of a different department.
1248
1249 At Level 1, the risk executive functional role is responsible for serving as a common C-SCRM
1250 resource for executive leadership and authorizing officials across the organization. Effective C-
1251 SCRM requires the risk executive to collaborate and gather perspectives from leaders such as the
1252 chief executive officer (CEO), chief risk officer (CRO), chief information officer (CIO), chief
1253 legal officer (CLO)/general counsel, chief information security officer (CISO), and chief
1254 acquisition officer (CAO). Organizations may form a C-SCRM council to collaborate on setting
1255 priorities and managing cyber supply chain risk for the organization. Through the risk framing
1256 process, these leaders are responsible for setting the direction for and approving the
1257 organization's C-SCRM organization-wide strategy. The C-SCRM strategy makes explicit the
1258 organization's assumptions, constraints, risk tolerances, and priorities/trade-offs.  These leaders
1259 are also responsible for developing and promulgating a holistic set of policies that span the
1260 organization's missions and business processes, guiding the establishment and maturation of a C-
1261 SCRM capability and the implementation of a cohesive set of C-SCRM activities. Leaders may
1262 elect to establish a C-SCRM PMO to drive C-SCRM activities and serve as a fulcrum for
1263 coordinated, C-SCRM-oriented services and guidance to the organization. Leaders should also
1264 clearly articulate lead roles at the mission and business process level responsible for detailing
1265 action plans and being accountable for the execution of C-SCRM activities.
1266
1267 Level 2 roles include but are not limited to representatives of each mission/business process
1268 including program managers, research and development, and acquisitions/procurement. Level 2
1269 C-SCRM activities address C-SCRM within the context of the organization's mission and
1270 business process. Mission and business process-specific strategies, policies, and procedures
1271 should be developed to tailor the C-SCRM implementation to fit the specific requirements of
1272 each mission and business process. Aligning to and building off of the high-level Enterprise
1273 Strategy and Implementation Plan, the organization should develop its own mission/business-
1274 level strategy and implementation plan and ensure C-SCRM execution within the constraints of
1275 its defined C-SCRM strategies, as well as awareness of and conformance to its C-SCRM
1276 policies. To facilitate the development and execution of Level 2 Strategy and Implementation
1277 plan(s), organizations may find benefit in forming a committee with representation from each
1278 mission/business process.  This coordination and collaboration can help to identify cyber supply
1279 chain risks within and across respective mission/business areas and to develop an enterprise and
1280 C-SCRM architecture that lends itself to risk-aware mission and business processes.  A C-SCRM
1281 PMO may also assist in the implementation of C-SCRM at Level 2 through the provision of
1282 services (e.g., policy templates, C-SCRM subject matter expert (SME) support).
1283
1284 Level 3 is comprised of personnel responsible for operational activities, including conducting
1285 procurements and executing system related C-SCRM activities as part of the organization's
1286 SDLC, which includes research and development, design, manufacturing, delivery, integration,
1287 operations and maintenance, and disposal/retirement of systems. These personnel include but are
1288 not limited to system owners, contracting officers, contracting officer representatives, architects,
1289 system integrators, and developers. These personnel are responsible for developing C-SCRM
1290 plans which address managing, ensuring the implementation, and monitoring of C-SCRM

1291   controls (to include those applicable to external parties, such as contractors) and the acquisition,
1292   development, and sustainment of systems across the SDLC to support mission and business
1293   processes. In organizations where a C-SCRM PMO has been established – activities such as
1294   product risk assessments may be provided as a centralized shared service.
1295
1296   Table 2-1 shows a summary of C-SCRM stakeholders for each level with the specific C-SCRM
1297   activities performed within the corresponding level. These activities are either direct C-SCRM
1298   activities or have an impact on C-SCRM.
1299
1300                   **Table 2-1: Cyber Supply Chain Risk Management Stakeholders**

| Levels | Level Name | Generic Stakeholder | Activities |
|--------|-----------|--------------------|------------|
| 1 | Organization | Executive Leadership (CEO, CIO, COO, CFO, CISO, Chief Technology Officer (CTO), CRO etc.) | Define Enterprise C-SCRM strategy and high-level implementation plan, policy, goals and objectives |
| 2 | Mission | Business Management (includes program management [PM], research and development [R&D], Engineering [SDLC oversight], Acquisition and Supplier Relationship Management/Cost Accounting, and other management related to reliability, safety, security, quality, C-SCRM PMO, etc.) | Develop mission and business process-specific strategy and policies and procedures, guidance and constraints, develop C-SCRM implementation plan(s) |
| 3 | Operational | Systems Management (architect, developers, system owner, QA/QC, test, and contracting personnel, approving selection, payment and approach for obtaining, maintenance engineering, disposal personnel, C-SCRM PMO staff, etc.) | Develop C-SCRM plans, implement policies and requirements, adhere to constraints provided by Levels 1 and 2 |

1301
1302
1303   The C-SCRM process should be carried out across the three risk management levels with the
1304   overall objective of continuous improvement in the organization's risk-related activities and
1305   effective inter-level and intra-level communication, thus integrating both strategic and tactical
1306   activities among all stakeholders with a shared interest in the mission/business success of the
1307   organization. Whether addressing a component, a system, a process, a mission process, or a
1308   policy, it is important to engage the relevant C-SCRM stakeholders at each level to ensure that
1309   risk management activities are as informed as possible.

1310
1311    The next few sections provide example activities in each level. Because each organization is
1312    different, however, there may be activities that are performed in different levels than listed as
1313    individual organizational context requires.
1314

> Section 4.5 provides a number of mission/business C-SCRM controls that organizations can
> tailor for their use to help guide Level 1, Level 2, and Level 3 C-SCRM activities. Note the
> tailoring should be scoped to the organization's risk management needs and organizations
> should analyze the cost of not implementing C-SCRM policies, capabilities, and controls
> when evaluating alternative risk response courses of action. These costs may include but are
> not limited to: poor quality or counterfeit products; supplier misuse of intellectual property;
> supplier tampering with or compromise of mission-critical information; and exposure to
> cyber-attacks through vulnerable supplier information systems.

1315
1316
1317    **2.1.2.  Level 1—Enterprise**
1318
1319    Level 1 (Enterprise) sets the tone and direction for organization-wide C-SCRM activities by
1320    providing an overarching C-SCRM strategy, C-SCRM policy, and High-Level Implementation
1321    Plan that shape how C-SCRM is implemented across the organization. Within Level-1,
1322    governance structures are formed to enable senior leaders and executives to collaborate on C-
1323    SCRM with the risk executive (function) in which leaders make C-SCRM decisions, delegate
1324    decisions to Levels 2 and 3, and prioritize organization-wide resource allocation for C-SCRM.
1325    Level 1 activities help to ensure that C-SCRM mitigation strategies are consistent with the
1326    strategic goals and objectives of the organization. Level 1 activities culminate in the C-SCRM
1327    Strategy, Policy, and High-Level Implementation Plan that shape and constrain how C-SCRM is
1328    carried out at Levels 2 and 3.
1329
1330    The C-SCRM governance structures and operational model dictate authority, responsibility, and
1331    decision-making power for C-SCRM and define 'how' C-SCRM processes are accomplished
1332    within the organization. The best C-SCRM governance and operating model is one that meets
1333    business and functional requirements of the organization. For example, an organization facing
1334    strict budgetary constraints or stiff C-SCRM requirements may consider governance and
1335    operational models which centralize decision-making authority and rely on a C-SCRM PMO to
1336    consolidate responsibilities for resource intensive tasks such as vendor risk assessments.  In
1337    contrast, organizations which have mission/business processes governed with a high degree of
1338    autonomy or possess highly differentiated C-SCRM requirements may opt for decentralized
1339    authority, responsibilities, and decision-making power.
1340
1341    In addition to defining C-SCRM governance structures and operating models, Level 1 carries out
1342    the activities necessary to frame C-SCRM for the organization. C-SCRM framing is the process
1343    by which the organization makes explicit the cyber supply chain risk assumptions (e.g., threats,
1344    vulnerabilities, risk impact, risk likelihood), constraints (e.g., organization policies, regulations,
1345    resource limitation, etc.), appetite and tolerance, and priorities and tradeoffs that guide C-SCRM
1346    decisions across the organization. The risk framing process provides the inputs necessary to
1347    establish the C-SCRM strategy that dictates how the organization plans to assess, responded to,

1348    and monitor cyber supply chain risk across the organization. A high-level implementation plan
1349    should also be developed to guide execution against the organization's C-SCRM strategy. The
1350    risk framing process is discussed in further detail within Appendix C of this document.
1351
1352    Informed by the risk framing process and the C-SCRM strategy, Level 1 provides the
1353    organization's C-SCRM policy. The C-SCRM policy establishes the C-SCRM program's
1354    purpose, outlines the organization's C-SCRM responsibilities, defines and grants authority to C-
1355    SCRM roles across the organization, and outlines applicable C-SCRM compliance and
1356    enforcement expectations and processes. Appendix C of this document provides example
1357    templates for the C-SCRM Strategy and C-SCRM Policy.
1358
1359    Risk assessment activities performed at Level 1 focus on assessing, responding to, and
1360    monitoring cyber supply chain risks to the organization's portfolio of operations, assets and
1361    personnel. Level 1 risk assessments may be based on the organization's Level 1 Frame step (i.e.,
1362    assumptions, constraints, appetite, tolerances, priorities and tradeoffs), or may be aggregated
1363    enterprise-level assumptions based on risk assessment completed across multiple mission and
1364    business processes. For example, a Level 1 risk assessment may analyze the exposure of the
1365    organization's primary mission or business objective to a threat scenario affecting a specific
1366    product or service provided through the supply chain. The enterprise-level risk determination
1367    may be based on an analysis of similar other analyses conducted within several mission and
1368    business processes as well as the relative criticality of those processes to the organization's
1369    primary objective.
1370
1371    Level 1 activities ultimately provide the overarching context and boundaries within which the
1372    organization's mission and business processes manage cyber supply chain risk. Outputs from
1373    Level 1 (e.g., C-SCRM Strategy, C-SCRM Policy, Governance and Operating Model) are further
1374    tailored and refined within Level 2 to fit the context of each mission and business process. Level
1375    1 outputs should also be iteratively informed by and updated as a result of C-SCRM outputs at
1376    lower levels.
1377
1378    *Additional information can be found in:  SR-1, SR-3, PM-2, PM-6, PM-7, PM-9, PM-28, PM-29,*
1379    *PM-30, and PM-31*
1380
1381    **2.1.3.  Level 2—Mission/Business Process**
1382
1383    Level 2 addresses how the organization assesses, responds to, and monitors cyber supply chain
1384    risk within mission and business processes. Level 2 activities are performed in accordance with
1385    the C-SCRM strategy, and policies provided by Level 1.[15] In this level, process-specific C-
1386    SCRM strategies, policies, and implementation plans dictate how the organization's C-SCRM
1387    goals and requirements are met within each mission and business process. Here, specific C-
1388    SCRM program requirements are defined and managed – including cost, schedule, performance,
1389    security, and a variety of critical nonfunctional requirements. These nonfunctional requirements
1390    include concepts such as reliability, dependability, safety, security, and quality.
1391

---

[15] For more information, see [NIST SP 800-39 Section 2.2].

1392    Many threats *to* and *through* the supply chain are addressed at this level in the management of
1393    third-party relationships with suppliers, developers, system integrators, external system service
1394    providers, and other ICT/OT-related service providers.  Because C-SCRM can both directly and
1395    indirectly impact mission and processes, understanding, integrating and coordinating C-SCRM
1396    activities at this level are critical for ensuring successful mission and business process
1397    operations. Level 2 activities focus on tailoring and applying the organization's C-SCRM frame
1398    to fit the specific mission and business process threats, vulnerabilities, impacts, and likelihoods.
1399    Informed by outputs from Level 1 (e.g., C-SCRM strategy), mission and business processes will
1400    adopt a C-SCRM strategy which tailors the organization's overall strategy to the specific mission
1401    and business process. At Level 2, the organization may also issue mission and business process
1402    specific policies which contextualize the organization's policy for the process.
1403
1404    In accordance with the C-SCRM strategy, organization leaders for specific mission and business
1405    processes should develop and execute a C-SCRM implementation plan. The C-SCRM
1406    implementation plan provides a more detailed roadmap for operationalizing the C-SCRM
1407    strategy(ies) within the mission and business process. Within the C-SCRM implementation
1408    plans, the mission and business process will specify C-SCRM roles and responsibilities,
1409    implementation milestones and dates, as well as processes for monitoring and reporting.
1410    Appendix D of this document provides example templates for the C-SCRM Strategy and
1411    Implementation Plan, as well as the C-SCRM Policy.
1412
1413    C-SCRM activities performed at Level 2 focus on assessing, responding to, and monitoring risk
1414    exposure arising from the mission and business process dependencies on suppliers, developers,
1415    system integrators, external system service providers, and other ICT/OT-related service
1416    providers. Risk exposures to the supply chain may arise as a result of primary dependencies on
1417    the supply chain or from secondary dependencies of the process on individual information
1418    systems or other mission and business processes.  For example, risk exposure may arise due to a
1419    supplier that provides critical system components or services to multiple information systems
1420    that critical processes depend on. Organizations must also consider as a source of risk the
1421    products and services unrelated to information systems that vendors provide as well as the role
1422    these products and services play in overall mission and business process objectives.
1423
1424    Outputs from Level 2 activities will have a significant impact in shaping how C-SCRM activities
1425    are carried out within Level 3. For example, risk tolerance and common control baseline
1426    decisions may be defined at Level 2, then tailored and applied within the context of individual
1427    information systems within Level 3.  Level 2 outputs should also be used to iteratively influence
1428    and further refine Level 1 outputs.
1429
1430    *Additional information can be found in:  SR-1, SR-3, SR-6, PM-2, PM-6, PM-7, PM-30, PM-31,*
1431    *and PM-32.*
1432
1433

1434  **2.1.4.  Level 3—Operational**
1435
1436  Within Level 3, outputs provided by C-SCRM activities completed at Levels 1 and 2 prepare the
1437  organization to execute C-SCRM at the operational-level in accordance with the RMF [NIST
1438  800-37r2]. C-SCRM is applied to information systems through the development and
1439  implementation of C-SCRM plans. These plans are heavily influenced by cyber supply chain risk
1440  assumptions, constraints, risk appetite and tolerance, and priorities and tradeoffs defined by
1441  Levels 1 and 2. C-SCRM plans dictate how C-SCRM activities are integrated into all systems in
1442  the SDLC, which includes acquisition  (both custom and off-the-shelf), requirements,
1443  architectural design, development, delivery, installation, integration, maintenance, and
1444  disposal/retirement. In general, C-SCRM plans are implementation specific, and provide policy
1445  implementation, requirements, constraints, and implications for systems that support mission and
1446  business process.
1447
1448  Level 3 activities focus on managing operational-level risk exposure resulting from any ICT/OT-
1449  related products and services provided through the supply chain that are in use by the
1450  organization or fall within the scope of the systems authorization boundary. Level 3 C-SCRM
1451  activities begin with an analysis of the likelihood and impact of potential cyber supply chain
1452  threats exploiting an operational-level vulnerability (i.e., in a system or system component).
1453  Where applicable, these risk assessments should be informed by risk assessments completed in
1454  Levels 1 and 2. In response to determined risk, organizations should evaluate alternative courses
1455  of action for reducing risk exposure (e.g., accept, avoid, mitigate, share and/or transfer). Risk
1456  response is achieved by selecting, tailoring, implementing, and monitoring C-SCRM controls
1457  throughout the SLDC in accordance with the RMF [NIST 800-37r2]. Selected C-SCRM controls
1458  often consist of a combination of inherited common controls from Levels 1 and 2 as well as
1459  information system-specific controls.
1460
1461  A key Level 3 activity is the development of the C-SCRM plan. Along with applicable security
1462  control information, the C-SCRM plan includes information on the system, its categorization,
1463  operational status, related agreements, architecture, key system personnel, related laws,
1464  regulations and policies, and contingency plan. This plan is a living document that should be
1465  maintained and used as the reference for continuous monitoring of implemented C-SCRM
1466  controls.
1467
1468  Information gathered as part of Level 3 C-SCRM activities should iteratively inform C-SCRM
1469  activities completed within Levels 1 and 2 to further refine C-SCRM strategies and
1470  implementation plans.
1471
1472  *Additional information can be found in:  SR-1, SR-2, SR-6, PL-2, PM-31, and PM-32.*
1473
1474  **2.1.5.  C-SCRM PMO**
1475
1476  A variety of operating models (e.g., centralized, decentralized, hybrid) are available to
1477  organizations that facilitate C-SCRM activities across the organization and its missions/business
1478  processes. One such model involves concentrating and assigning responsibilities for certain C-
1479  SCRM activities to a central PMO. In this model, the C-SCRM PMO acts as a service provider

1480 to other missions/business processes. Missions/business processes are then responsible for
1481 selecting and requesting services from the C-SCRM PMO as part of their responsibilities to meet
1482 the organization's C-SCRM goals and objectives.  There are a variety of beneficial services that
1483 a PMO may provide:

1484  &bull; Advisory services and subject eatter Expertise
1485  &bull; Chair for internal C-SCRM working groups/coordination bodies
1486  &bull; Centralized hub for tools, job aids, awareness and training templates
1487  &bull; Supplier/product risk assessments
1488  &bull; Liaison to external stakeholders
1489  &bull; Information sharing management (e.g., to/from FASC)
1490  &bull; Management of C-SCRM risk register
1491  &bull; Secretariat/staffing function for enterprise C-SCRM governance
1492  &bull; C-SCRM project and performance management
1493  &bull; C-SCRM Briefings, Presentations, and Reporting
1494

1495 A C-SCRM PMO typically consists of C-SCRM SMEs who help drive the C-SCRM strategy
1496 and implementation across the organization and its mission and business processes. A C-SCRM
1497 PMO may include or report to a dedicated executive-level official responsible for overseeing C-
1498 SCRM activities across the organization. Depending on organization-specific constraints, a C-
1499 SCRM PMO may consist of dedicated personnel or include matrixed representatives with
1500 responsibilities for C-SCRM from several of the organization's processes including, but not
1501 limited to information security, procurement, risk management, engineering, software
1502 development, IT, legal, and HR.
1503

1504 The C-SCRM PMO responsibilities may include providing services to the organization's leaders
1505 that help set the tone for how C-SCRM is applied throughout the organization. The C-SCRM
1506 PMO may provide SME support to guide Level 1 stakeholders through the risk framing process
1507 which includes establishing the organizational appetite and tolerance for cyber supply chain risk.
1508 In addition, accountable risk executives may delegate responsibility for drafting the organization
1509 C-SCRM strategy and policy to the PMO. C-SCRM PMOs may also coordinate C-SCRM
1510 information-sharing interagency across the supply chain and across the organization mission and
1511 business processes. Finally, the PMO may conduct C-SCRM-focused executive-level briefings
1512 (e.g., to the risk executive function, board of directors) to help Level 1 stakeholders develop an
1513 aggregated picture of the state of cyber supply chain risk across the organization.
1514

1515 At Level 2, C-SCRM PMO may develop C-SCRM starter kits which contain a base strategy, set
1516 of policies, procedures and guidelines which can be further customized within specific mission
1517 and business processes.  This PMO may also provide SME consulting support to stakeholders
1518 within mission and business processes as they create process-specific C-SCRM strategies and
1519 develop C-SCRM implementation plans. As part of this responsibility, the C-SCRM PMO may
1520 advise on or develop C-SCRM common control baselines within the organization mission and
1521 business processes. The C-SCRM PMO may also perform C-SCRM risk assessments focused on
1522 suppliers, developers, system integrators, external system service providers, and other ICT/OT-
1523 related service providers of both technology and non-technology related products and services.
1524

1525   The responsibility of a C-SCRM PMO at Levels 1 and 2 would ultimately influence C-SCRM
1526   activities at the Level 3 operational level. A C-SCRM PMO may advise teams throughout the
1527   SDLC on C-SCRM control selection, tailoring, and monitoring. Ultimately a C-SCRM PMO
1528   may be responsible for activities that produce C-SCRM outputs across the risk management
1529   levels. Centralizing C-SCRM services offers organizations an opportunity to capitalize on
1530   specialized skill sets within a consolidated team that offers high quality C-SCRM services to the
1531   rest of the organization. By centralizing risk assessment services – organizations may achieve a
1532   level of standardization not otherwise possible (e.g., in a decentralized model). Organizations
1533   may also realize cost efficiencies in cases where PMO resources are dedicated to C-SCRM
1534   activities versus resources in decentralized models which may perform multiple roles in addition
1535   to C-SCRM responsibilities.
1536
1537
1538

## 3. CRITICAL SUCCESS FACTORS

To successfully address evolving cyber supply chain risks, organizations need to engage multiple internal processes and capabilities, communicate and collaborate across organizational levels and mission areas, and ensure that all individuals within the organization understand their role in managing cyber supply chain risks. Organizations need strategies for communicating, determining how best to implement, and monitoring the effectiveness of their supply chain cybersecurity controls and practices. In addition to communicating cyber supply chain controls internally, organizations should engage with peers to exchange cyber supply chain risk management insights. These insights will aid organizations in continuously evaluating how well they are doing and identify where they need to improve and how to take steps to mature their C-SCRM program. This section addresses the requisite organizational processes and capabilities to make C-SCRM successful.

### 3.1.    C-SCRM in Acquisition

Integrating C-SCRM considerations into acquisition activities is essential to improving management of cyber supply chain risks at every step of the procurement and contract management process. This life cycle begins with a purchaser identifying a need, includes the processes to plan for and articulate requirements, conduct research to identify and assess viable sources of supply, solicit bids and evaluate offers, to include ensuring conformance to C-SCRM requirements and assessing C-SCRM risk associated with the bidder and the proposed product and/or service offering.  After contract award, ensure the supplier satisfies the terms and conditions articulated in their contractual agreement and that the products and services conform as expected and required.  C-SCRM considerations need to be addressed at every step in this life cycle.

Organizations rely heavily on commercial products and outsourced services to perform operations and fulfill their missions and business objectives. In addition to addressing cyber supply chain risks and performing C-SCRM activities during each phase of the acquisition process, organizations should develop and execute an acquisition strategy that drives forward reductions in their overall cyber supply chain risk exposure. Through such strategies, organizations can reduce cyber supply chain risks within specific procurement processes as well as for the overall enterprise. Adopting acquisition policies and processes that integrate C-SCRM will then aid, direct, and inform the organization's efforts to implement those strategies and realize targeted risk-reducing outcomes which align and lead to achievement of the organization's C-SCRM strategic goals and objectives.

Additionally, adopting C-SCRM controls aligned to an industry-recognized set of standards and guidelines (e.g., NIST 800-53 Rev.5, NIST CSF), the organization can ensure holistic coverage of cyber supply chain risks and corresponding C-SCRM practices. C-SCRM controls may apply to different participants of the supply chain to include the organization itself, prime contractors, and sub-contractors.  Because organizations heavily rely on prime contractors and their subcontractors to develop and implement ICT products and services, those controls that are implemented within the SDLC are likely to flow down to subcontractors.  Establishing C-SCRM controls that apply throughout the supply chain and the SDLC will aid the organization in

1584    establishing common expectations and lexicon with suppliers and sub-suppliers to help all
1585    participants manage cyber supply chain risks to and through the supply chain.
1586
1587    **3.1.1. Acquisition in the C-SCRM Strategy and Implementation Plan**
1588
1589    An organization's C-SCRM Strategy and Implementation Plan serve as the roadmap to guide the
1590    organization toward achievement of long-term, sustainable reductions in cyber supply chain risk
1591    exposure. As a core part of the C-SCRM Strategy and Implementation Plan, organizations should
1592    address how cyber supply chain risks are managed throughout the acquisition process.

1593    Cyber supply chain risks include those arising from the supplier's organization, products or
1594    services, as well as the supplier's own suppliers and supply chains. The C-SCRM PMO may be
1595    helpful in developing specific strategies and implementation plans for integrating C-SCRM
1596    considerations into acquisitions. Acquisition activities relevant to C-SCRM include, but are not
1597    limited to:

1598    • Promoting awareness and communicating C-SCRM expectations as part of supplier
1599      relationship management efforts;
1600    • Establishing a checklist of acquisition security requirements that must be completed as
1601      part of procurement requests to ensure necessary provision and protections are in place;
1602    • Leveraging an external shared service provider or utilize the C-SCRM PMO to provide
1603      supplier, product, and/or services assessment activities as a shared service to other
1604      internal processes including acquisition;
1605    • Conducting robust due diligence to inform determinations about a bidder's responsibility
1606      and to identify and assess bidders' cyber supply chain risk posture or risk associated with
1607      a given product or service offering;
1608    • Including C-SCRM criteria in source selection evaluations;
1609    • Establishing and referencing a list of prohibited suppliers, if appropriate, per applicable
1610      regulatory and legal references; and
1611    • Establishing and procuring from an approved products list or list of preferred or qualified
1612      suppliers who have demonstrated conformance with the organization's security
1613      requirements through a rigorous process defined by the organization or another
1614      acceptable qualified list program activity.

1615    The C-SCRM Strategy and Implementation Plan should address the acquisition security-relevant
1616    foundational elements necessary to implement a C-SCRM program. To support the strategy,
1617    organization leaders should promote the value and importance of C-SCRM within acquisitions
1618    and ensure sufficient, dedicated funding is in place for necessary activities. Doing so will help
1619    organizations ensure responsibility for program processes and accountability for progress toward
1620    the attainment of results. Organizations should also assign roles and responsibilities, some of
1621    which will be cross-organizational in nature and team-based, while others will be specific to
1622    acquisition processes. Finally, relevant training should be provided to members of the acquisition
1623    workforce to ensure roles and responsibilities are understood and executed in alignment with
1624    leader expectations.

1625    The organization's capabilities, resources, operational constraints and existing portfolio of
1626    supplier relationships, contracts, acquired services and products provide the baseline context
1627    necessary to lay out a strategic path that is realistic and achievable. This baseline starting point
1628    also serves as a marker from which performance progress and outcomes can be tracked and
1629    assessed.

1630    A critical first step is to ensure there is a current and accurate inventory of the organization's
1631    supplier relationships and contracts as well as an understanding of the products or services those
1632    suppliers provide. This information allows for a mapping of these suppliers into strategically
1633    relevant groupings. For example, an assessment of these suppliers might result in a grouping of
1634    them into categories (e.g., "strategic/innovative," "mission-critical," "sustaining" or
1635    "standard/non-essential"). This segmentation facilitates further analysis and understanding of the
1636    exposure to cyber supply chain risk throughout the organization, and helps to focus priority
1637    attention on those critical suppliers that are of the most strategic or operational importance to the
1638    organization and its mission and business processes. It is useful to identify which products and
1639    services require a higher level of confidence that risk is minimized, and can be helpful in
1640    identifying areas of risk, such as overreliance on a single source of supply. This inventory and
1641    mapping also facilitates the selection and tailoring of C-SCRM contract language and evaluation
1642    criteria.

1643    *Additional information can be found in:  SA-1, SA-2, SA-4, SR-5, SR-13, and NISTIR 8179[1]*
1644
1645    **3.1.2.  The Role of C-SCRM in the Acquisition Process**
1646
1647    When conducting a procurement, organizations should designate experts from different subject
1648    matter areas to participate in the acquisition process as members of the Acquisition Team.
1649    While procurement requirements address and are tailored to satisfying a specific purpose and
1650    ensure compliance mandates are met, contextual factors such as mission criticality, sensitivity of
1651    data, and the operational environment must also be considered to effectively address cyber
1652    supply chain risk.

1653    This contextual basis sets the stage for the Acquisition Team to be able to effectively gauge their
1654    tolerance for risk as it pertains to a specific procurement requirement and determine which of the
1655    [NIST SP 800-161 Rev 1] and [NIST SP 800-53 Rev 5] controls are relevant and necessary to
1656    consider for specific acquisitions. The program office – or requiring official – should consult
1657    with information security personnel to complete this control selection process and work with
1658    their procurement official to incorporate these controls into requirements documents and
1659    contracts. Security is a key factor in procurement decisions.

1660    Acquisition policies and processes need to incorporate C-SCRM considerations into each step of
1661    the procurement and contract management life cycle management process (i.e., plan
1662    procurement, define/develop requirements, perform market analysis, complete procurement,
1663    ensure compliance, monitor performance and for changes that affect C-SCRM risk status) as
1664    described in [NISTIR 7622]. During the 'plan procurement' step, the criticality of the good or
1665    service to be procured needs to be identified, along with a description of the factors that are
1666    driving the determination of the level of criticality. This activity is typically led by the

1667 procurement official with the help from officials across the organization including but not
1668 limited to mission/business representatives, information security, and legal.

1669 Once a procurement plan is in place, the organization should develop and define requirements.
1670 Requirements should be developed and refined to address cyber supply chain risks, in addition to
1671 specifying performance, schedule, and cost objectives. This process is typically initiated by the
1672 acquirer mission/business process owner or a designee in collaboration with the procurement
1673 official and other members of the C-SCRM team.

1674 With requirements defined, organizations will typically complete a market analysis for potential
1675 suppliers. Market research and analysis activities will explore the availability of potential or pre-
1676 qualified sources of supply. This step is typically initiated by the acquirer mission and business
1677 process owner or a designated representative. Organizations should use this phase to conduct
1678 more robust due diligence research on potential suppliers and/or products in order to generate a
1679 supplier risk profile. As part of due diligence, the organization may consider the market
1680 concentration for the sought-after product or service as a means of identifying interdependencies
1681 within the supply chain. The organization may also use a request for information (RFIs) and/or
1682 due diligence questionnaires for the initial screening and collection of evidence from potential
1683 suppliers. Organizations should not treat the initial C-SCRM due diligence risk assessment as
1684 exhaustive. Results of this research can also be helpful in shaping the sourcing approach and
1685 refining requirements.

1686 Finally, the organization will complete the procurement step by releasing a statement of work
1687 (SOW) or statement of objective (SOO) for the release of a request for proposal (RFP), or
1688 request for quotes (RFQ). As part of selection, any bidders responding to the RFP or RFQ should
1689 be evaluated against relevant, key C-SCRM criteria. The RFP review process should also include
1690 any procurement-specific supplier risk assessment. The assessment criteria will be heavily
1691 informed by the defined C-SCRM requirements and include coverage over but not limited to
1692 information about the organization, its security processes, and its security track record. The
1693 response review process involves multiple C-SCRM stakeholders including procurement, the
1694 mission and business process owner, as well as appropriate information system owners and
1695 technical experts. Once selection has occurred, organizations should complete product or system
1696 component risk assessments with coverage over, but not limited to the products or system
1697 components quality, vulnerability, and authenticity.

1698 Once the contract is executed, the organization should monitor for change that alters its cyber
1699 supply chain risk exposure. Change that alters cyber supply chain risk exposure may include but
1700 is not limited to internal organization or system changes, supplier operational or structural
1701 changes, as well as geopolitical or environmental changes. An organization should continuously
1702 apply lessons learned collected during the acquisition process to enhance its ability to assess,
1703 respond to and monitor cyber supply chain risk within its supply chain.

1704 Table 3-1 shows a summary of where C-SCRM assessments may take place within the various
1705 steps of the procurement process.

1706                    **Table 3-1: C-SCRM in the Procurement Process**

| Procurement Process | Service Risk Assessment | Supplier Risk Assessment | Product Risk Assessment |
|---|---|---|---|
| **Plan Procurement** | Service Risk Assessment Criticality of Needed Service Other Context (functions performed; access to systems/data, etc.) Fit for Purpose | Fit for Purpose | Criticality of Needed Product Other Context (Operating Environment, Data, Users, etc.) Fit for Purpose |
| **Define/Develop Requirements** | Select applicable C-SCRM controls/ requirements | Select applicable C-SCRM controls/ /requirements | Select applicable C-SCRM controls/ requirements |
| **Perform Market Analysis** | | Initial Risk Assessment (e.g., Due-Diligence Questionnaires) | Research product options and risk factors |
| **Solicit Bids/ Complete Procurement** | | Complete Risk Assessment | Pre-Deployment Risk Assessment |
| **Operate & Maintain** | Continuous Risk Monitoring | Continuous Risk Monitoring | Continuous Risk Monitoring |

1707

1708   In addition to process activities, there are many useful acquisition security-enhancing tools and
1709   techniques available, including: obscuring the end use of a system or system component; using
1710   blind or filtered buys; requiring tamper-evident packaging; or using trusted or controlled
1711   distribution. The results from a supply chain risk assessment can guide and inform the strategies,
1712   tools, and methods that are most applicable to the situation. Tools and techniques may provide
1713   protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion
1714   of malicious software or backdoors, and poor development practices throughout the system
1715   development life cycle.

1716   To ensure effective and continued management of cyber supply chain risks throughout the
1717   acquisition lifecycle, contractual agreements and contract management should include:
1718     • The satisfaction of applicable security requirements in contracts and mechanisms as a
1719        qualifying condition for award;
1720     • Flow-down control requirements to sub-contractors, if and when applicable, including C-
1721        SCRM performance objectives, linked to method of inspection, in a Quality Assurance
1722        Surveillance Plan;
1723     • Periodic re-validation of supplier adherence to security requirements to ensure continual
1724        compliance;
1725     • Processes and protocols for communication and reporting of information about
1726        vulnerabilities, incidents, and other business disruptions, to include acceptable deviations if
1727        the business disruption is serious enough and baseline criteria to determine whether a
1728        disruption qualifies as serious ; and
1729     • Terms and conditions that address government, supplier, and other applicable third
1730        party(ies) roles, responsibilities, and actions for responding to identified supply chain

1731    risk(s), or risk incident(s), in order to mitigate risk exposure, minimize harm, and support
1732    timely corrective action or recovery from an incident.
1733

1734  There are a variety of acceptable validation and re-validation methods, such as required
1735  certifications, site visits, third-party assessment, or self-attestation. The type and rigor of required
1736  methods should be commensurate to the criticality of the service or product being acquired and
1737  the corresponding assurance requirements.
1738

1739  Additional guidance for integrating C-SCRM into the acquisition process is provided in
1740  Appendix C that demonstrates the enhanced overlay of C-SCRM into the NIST SP 800-39 Risk
1741  Management Process. In addition, organizations should refer to and follow
1742  acquisition/procurement policies, regulations, and best practices that are specific to their domain
1743  (e.g., critical infrastructure sector, State Government, etc.)

1744  *Additional information can be found in:  SA-1, SA-2, SA-3, SA-4, SA-9, SA-19, SA-20, SA-22, SR-*
1745  *5, SR-6, SR-10, and SR-11*

## 3.2.    Supply Chain Information Sharing

1746
1747
1748  Organizations are continuously exposed to risk originating from their supply chains. An effective
1749  information-sharing process helps to ensure organizations can gain access to information critical
1750  to understanding and mitigating cyber supply chain risks, and also share relevant information to
1751  others that may benefit from or require knowing about these risks.
1752
1753  To aid in identifying, assessing, monitoring, and responding to cyber supply chain risks,
1754  organizations should build information-sharing processes and activities into their C-SCRM
1755  programs. This may include establishing information-sharing agreements with peer
1756  organizations, as well as with business partners and suppliers.  By exchanging supply chain risk
1757  information within a sharing community, organizations can leverage the collective knowledge,
1758  experience, and capabilities of that sharing community to gain a more complete understanding of
1759  the threats the organization may face. Additionally, sharing of supply chain risk information
1760  allows organizations to better detect campaigns that target specific industry sectors and
1761  institutions.
1762
1763  Federal organizations should establish processes to be able to effectively engage with the
1764  FASC's information sharing agency, which is responsible for facilitating information sharing
1765  among government agencies and acts as a central, government-wide facilitator for C-SCRM
1766  information sharing activities.
1767
1768  NIST SP 800-150 describes key practices for establishing and participating in supply chain risk
1769  information-sharing relationships as follows:
1770    • Establish information sharing goals and objectives that support business processes and
1771      security policies
1772    • Identify existing internal sources of supply chain risk information
1773    • Specify the scope of information sharing activities
1774    • Establish information sharing rules

1775    • Join and participate in information sharing efforts
1776    • Actively seek to enrich indicators by providing additional context, corrections, or
1777      suggested improvements
1778    • Use secure, automated workflows to publish, consume, analyze, and act upon supply
1779      chain risk information
1780    • Proactively establish supply chain risk information sharing agreements
1781    • Protect the security and privacy of sensitive information
1782    • Provide ongoing support for information sharing activities.

1783    As shown in Table 3-2, below, supply chain risk information describes or identifies cyber supply
1784    chain relevant characteristics and risk factors associated with a product or service or source of
1785    supply. It may exist in various forms (e.g., raw data, a supply chain network map, risk
1786    assessment report, etc.) and should be accompanied with the metadata that will facilitate an
1787    assessment of a level of confidence in and credibility of the information.  Organizations should
1788    follow established processes and procedures that describe whether and when sharing or reporting
1789    of certain information is mandated or voluntary and if there are any necessary requirements with
1790    which to adhere regarding information handling, protection and classification.
1791

1792
1793

**Table 3-2: Cyber Supply Chain Characteristics and Risk Factors Associated with a Product, Service, or Source of Supply[16]**

| Source of Supply, Product, or Service Characteristics | Risk Indicators, Analysis, and Findings |
| --- | --- |
| <ul><li>Features and functionality;</li><li>Access to data and information, including system privileges;</li><li>Installation or Operating Environment;</li><li>Security, authenticity, and integrity of a given product or service and the associated supply and compilation chain;</li><li>The ability of the source to produce and deliver a product or service, as expected;</li><li>Foreign control of, or influence over, the source (e.g., foreign ownership, personal and professional ties between the source and any foreign entity, legal regime of any foreign country in which the source is headquartered or conducts operations);</li><li>Market alternatives to the source; and</li><li>Potential risk factors such as geo-political, legal, managerial/internal controls, financial stability, cyber incidents, personal and physical security, or any other information that would factor into an analysis of the security, safety, integrity, resilience, reliability, quality, trustworthiness, or authenticity of a product, service or source.</li></ul> | <ul><li>Threat information include indicators (system artifacts or observables associated with an attack), tactics, techniques, and procedures (TTPs);</li><li>Security alerts, threat intelligence reports;</li><li>Implications to national security, homeland security, and/or national critical processes associated with use of the product or service;</li><li>Vulnerability of federal systems, programs, or facilities;</li><li>Threat level and vulnerability level assessment/score;</li><li>Potential impact or harm caused by the possible loss, damage, or compromise of a product, material, or service to an organization's operations or mission and likelihood of a potential impact or harm, or the exploitability of a system; and</li><li>Capacity to mitigate risks identified.</li></ul> |

1794
1795
1796     **3.3.    C-SCRM Training and Awareness**
1797
1798     Numerous individuals within the organization contribute to the success of C-SCRM.  These may
1799     include but are not limited to information security, procurement, risk management, engineering,
1800     software development, IT, legal, HR. Examples of these contributions include:

---

[16] Cyber Supply Chain Characteristics and Risk Factors Associated with a Product, Service, or Source of Supply is non-exhaustive.

1801     •    System Owners are responsible for multiple facets of C-SCRM at the operational-level as
1802          part of their responsibility for the development, procurement, integration, modification,
1803          operation, maintenance, and/or final disposition of an information system;
1804     •    Human Resources defines and implements background checks and training policies
1805          which help ensure that individuals are trained in appropriate C-SCRM processes and
1806          procedures;
1807     •    Legal helps draft C-SCRM-specific contractual language that is included by procurement
1808          in contracts with suppliers, developers, system integrators, external system service
1809          providers, and other ICT/OT-related service providers;
1810     •    Acquisition/procurement defines the process for implementing supplier assurance
1811          practices embedded in the acquisition process;
1812     •    Engineering designs products and must understand existing requirements for use of open-
1813          source components;
1814     •    Software developers ensure software vulnerabilities are identified and addressed as early
1815          as possible, including testing and fixing the code;
1816     •    Shipping and receiving ensures that boxes that contain critical components have not been
1817          tampered with en route or at the warehouse.

1818 Everyone within an organization has a role in managing cyber supply chain risks. The
1819 organizations should foster an overall culture of security including C-SCRM as an integral part.
1820 The organizations can use a variety of communication methods to foster the culture, of which
1821 traditional awareness and role-based training are only one component.

1822 Every individual within an organization should receive appropriate training to help them
1823 understand the importance of C-SCRM for their organization, their specific roles and
1824 responsibilities, and processes and procedures for reporting incidents. This training can be
1825 integrated into the overall cybersecurity awareness training.

1826 Those individuals who have more significant roles in managing cyber supply chain risk should
1827 receive tailored C-SCRM training that helps them understand the scope of their responsibilities,
1828 specific processes and procedures they are responsible for implementing, and what actions to
1829 take in case of an incident, disruption, or another C-SCRM-related event. The organizations
1830 should establish specific role-based training criteria and develop role-specific C-SCRM training
1831 to address specific C-SCRM roles and responsibilities. The organizations may also consider
1832 adding C-SCRM content into already existing role-based training for some specific roles.  Refer
1833 to the Awareness and Training controls in Section 4.5 for more detail.

1834 Organizations should consider use of the NIST National Initiative for Cybersecurity Education
1835 (NICE) Framework[17] as a means of forming a common lexicon on C-SCRM workforce topics.
1836 This will aid organizations in developing training linked to role-specific C-SCRM
1837 responsibilities and communicating cybersecurity workforce-related topics. The NICE
1838 Framework outlines Categories, Specialty Areas, Work Roles, KSAs (Knowledge, Skills, and
1839 Abilities), and Tasks which describe cybersecurity work.

1840

---

[17] NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

1841　**3.4.　Capability Implementation Measurement and C-SCRM Metrics**
1842

1843　Organizations should actively manage the efficiency and effectiveness of their C-SCRM
1844　programs through ongoing measurement of the programs themselves. Organizations can use
1845　several methods of measuring and managing the effectiveness of their C-SCRM program:

1846　• Using a framework, such as NIST CSF to assess their C-SCRM capabilities
1847　• Measuring progress of their C-SCRM initiatives towards completion
1848　• Measuring performance of their C-SCRM initiatives towards desired outcomes

1849　All methods rely on a variety of data collection, analysis, contextualization, and reporting
1850　activities.  Collectively, these methods should be used to track and report out progress and results
1851　that ultimately indicate reductions in risk exposure and improvements in the organization's
1852　security outcomes.

1853　C-SCRM performance management provides a number of organizational and financial benefits.
1854　Major benefits include increasing stakeholder accountability for C-SCRM performance;
1855　improving effectiveness of C-SCRM activities; demonstrating compliance with laws, rules and
1856　regulations, providing quantifiable inputs for resource allocation decisions, cost-avoidance
1857　associated with reduced impact from—or likelihood of experiencing—a cyber-supply chain
1858　incident.

1859　Organizations can use a framework such as NIST CSF Implementation Tiers to baseline their C-
1860　SCRM capabilities.  Frameworks such as this provide a useful context for an organization to
1861　track and gauge the increasing rigor and sophistication of their C-SCRM practices. Progression
1862　against framework topics is measured using ordinal (i.e., 1-5) scales which illustrate the
1863　progression of capabilities across tiers. The following are examples of how C-SCRM capability
1864　could be gauged by applying NIST CSF Tiers:
1865

1866　• CSF Tier 1: The organization does not understand its cyber supply chain risks or its role
1867　　in the larger ecosystem. The organization does not collaborate with other entities or have
1868　　processes in place to identify, assess and mitigate its cyber supply chain risks.

1869　• CSF Tier 2: The organization understands its cyber supply chain risks associated with
1870　　products and services and its role in the larger ecosystem. The organization has not
1871　　formalized its capabilities to manage cyber supply chain risks internally or its capability
1872　　to engage and share information with entities in the broader ecosystem.

1873　• CSF Tier 3: Organization-wide approach to managing cyber supply chain risks is enacted
1874　　via enterprise risk management policies, processes, and procedures. This likely includes a
1875　　governance structure (e.g., Risk Council) that manages cyber supply chain risks in
1876　　balance with other enterprise risks. Policies, processes, and procedures are implemented
1877　　consistently, as intended, and continuously monitored and reviewed. Personnel possess
1878　　the knowledge and skills to perform their appointed cyber supply chain risk management
1879　　responsibilities. The organization has formal agreements in place to communicate
1880　　baseline requirements to its suppliers and partners. The organization understands its
1881　　external dependencies and collaborates with partners to share information to enable risk-

1882    based management decisions within the organization in response to events.

1883    • CSF Tier 4: The organization actively consumes and distributes information with partners
1884       and uses real-time or near real-time information to improve cybersecurity and supply
1885       chain security before an event occurs. The organization leverages institutionalized
1886       knowledge of cyber supply chain risk management with its external suppliers and
1887       partners as well as internally, in related functional areas and at all levels of the
1888       organization. The organization communicates proactively using formal (e.g., agreements)
1889       and informal mechanisms to develop and maintain strong relationships with its suppliers,
1890       buyers, and other partners.

1891    Capability building begins by establishing a solid programmatic foundation that includes
1892    enabling strategies and plans, policies and guidance, investment in training and dedicated
1893    program resources. Once this foundational capability is in place, organizations can use these
1894    progression charts to orient the strategic direction of their programs to target states of C-SCRM
1895    capability in different areas of the program. Table 3-3 provides an example C-SCRM
1896    implementation model.

1897

1898

1899 **Table 3-3: Example C-SCRM Practice Implementation Model[18]**

| Implementation Level | Associated C-SCRM Practices |
|---|---|
| Foundational | • Established C-SCRM Policies across enterprise-levels<br>• Defined C-SCRM hierarchy<br>• Established C-SCRM governance structure<br>• Well-documented, consistent C-SCRM processes<br>• Quality and reliability program<br>• Explicit roles for C-SCRM<br>• Adequate and dedicated C-SCRM resources<br>• Defined C-SCRM control baseline<br>• Established C-SCRM internal checks and balance to assure compliance<br>• Established supplier management program<br>• C-SCRM included in an established incident management program |
| Sustaining | • Use of third-party assessments, site visits, and formal certification<br>• Defined C-SCRM risk appetite and risk tolerances<br>• Formalized information sharing processes (e.g., engages w/ FASC)<br>• Formal C-SCRM training program<br>• C-SCRM integrated into SDLC<br>• C-SCRM integrated into contractual agreements<br>• Suppliers participate in incident response, disaster recovery, and contingency planning<br>• Formally defined, collected, and reported C-SCRM metrics |
| Enhancing | • C-SCRM process automation<br>• Use of quantitative risk analysis<br>• Predictive and adaptive C-SCRM strategies and processes |

1900

1901 **3.4.1.  Measuring C-SCRM Efficacy, Efficiency, and Compliance**

1902

1903 Organizations typically rely on information security measures to facilitate decision making as
1904 well as improve performance and accountability in their information security programs.
1905 Organizations can achieve similar benefits within their C-SCRM programs. Similar to
1906 information security measures, C-SCRM-focused measures can be obtained at different levels of
1907 an organization. NIST SP 800-55 provides guidance on the specific development, selection, and
1908 implementation of operational-level and program-level performance measures. Table 3-3
1909 provides example measurement topics across the three Risk Management levels.

---

[18] For more information on C-SCRM capabilities, refer to section 1.5 C-SCRM Key Practices.

1910          **Table 3-4: Example Measurement Topics Across the Risk Management Levels**

| Risk Level | Example Measurement Topics |
|---|---|
| Level 1 | • Policy adoption at lower levels<br>• Timeliness of policy adoption at lower levels<br>• Adherence to risk appetite and tolerance thresholds<br>• Differentiated levels of risk exposure across Level 2<br>• Compliance with regulatory mandates<br>• Adherence to customer requirements |
| Level 2 | • Effectiveness of mitigation strategies<br>• Time allocation across C-SCRM activities<br>• Mission/business process-level risk exposure<br>• Degree and quality of C-SCRM requirement adoption in mission/business processes<br>• Use of C-SCRM PMO by Level 3 |
| Level 3 | • Design effectiveness of controls<br>• Operating effectiveness of controls<br>• Cost-efficiency of controls |

1911

1912     Organizations may adopt a single or combination of methods to manage the effectiveness of their
1913     C-SCRM programs. NIST SP 800-55 Rev.1 articulates three different components of
1914     performance:

1915          • **Implementation:** Demonstrates the progress in implementing programs, controls, and
1916            associated policies and procedures;
1917          • **Effectiveness/Efficiency:** Provides insight whether programs, processes, and controls are
1918            implemented correctly, operate as intended, and meet desired outcomes;
1919          • **Impact:** Analyzes the impact of C-SCRM on broader objectives (e.g., contribution to
1920            business process cost savings; reduction in national security risk).

1921     **3.5.     Dedicated Resources**
1922

1923     To appropriately manage cyber supply chain risks, organizations should commit dedicated funds
1924     towards this effort. Identifying resource needs and taking steps to secure adequate, recurring, and
1925     dedicated funding is an essential and important activity that needs to be built into the C-SCRM
1926     strategy and implementation planning effort and incorporated into an organization's budgeting,
1927     investment review, and funds management processes. Access to adequate resources is a critical,
1928     key enabler for the establishment and sustainment of a C-SCRM program capability.  The
1929     continued availability of dedicated funds will allow organizations to sustain, expand, and mature
1930     their capabilities over time.
1931

1932    Securing and assigning C-SCRM funding is representative of leadership's commitment to the
1933    importance of C-SCRM and its relevance to national and economic security and ensuring the
1934    protection, continuity and resilience of mission and business processes and assets.
1935
1936    Funding facilitates goal and action-oriented planning. Examining resource needs and allocating
1937    funding prompts a budgeting and strategic planning process. Effective organizations begin by
1938    defining a set of goals and objectives upon which organizations should build a strategic roadmap
1939    laying out the path to achieve them, through the assignment and allocation of finite resources.
1940    The establishment of dedicated funding, tied to C-SCRM objectives, sets conditions for
1941    accountability for performance and compels responsible staff to be efficient and effective and to
1942    adopt a mindset of continuously seeking to improve C-SCRM capabilities and achieve security
1943    enhancing outcomes.
1944
1945    Obtaining new or increased funding can be a challenge as resources are often scarce and
1946    necessary for many competing purposes.  The limited nature of funds forces prioritization. C-
1947    SCRM leaders need to first examine what can be done within the constraints of existing
1948    resources and be able to articulate, prioritize, and defend their requests for additional resources.
1949    For new investment proposals, this requires a reconciliation of planned initiatives against the
1950    organization's mission/business objectives. When well-executed, a systematic planning process
1951    can tighten the alignment of C-SCRM processes to these objectives.
1952
1953    Many C-SCRM processes can and should be built into existing program and operational
1954    activities and may be able to be adequately performed using available funds. However, there may
1955    be a need for an influx of one-time resources to establish an initial C-SCRM program capability.
1956    For example, this might include the need to hire new personnel with expertise in C-SCRM, to
1957    acquire contractor support to aid in developing C-SCRM program guidance, or to develop
1958    content for role-based C-SCRM training. There may also be insufficient resources in place to
1959    satisfy all recurring C-SCRM program needs. Existing funds may need to be reallocated towards
1960    C-SCRM efforts or new or additional funds requested. Organizations should also seek out
1961    opportunities to leverage shared services whenever practical.
1962
1963    The use of shared services can optimize the use of scarce resources and concentrates capability
1964    into centers of excellence providing cost-efficient access to services, systems, or tools.
1965    Organizations pursuing shared service models for C-SCRM should also be aware of the
1966    challenges with such models. Shared services (e.g., C-SCRM PMO) are most effective when the
1967    organization at large relies on a fairly homogenous set of C-SCRM strategy, policies, and
1968    processes.  In many instances, centralized delivery of C-SCRM services require a robust
1969    technology infrastructure. The organization's systems should be able to support process
1970    automation and centralized delivery in order to fully realize the benefits of a shared services
1971    model.
1972
1973    Consultation with budget officials is critical to understanding what options may be available and
1974    viable in the near term and outyears. These officials can also advise on how best to justify needs,
1975    and the timeframes and processes for requesting new funds. There are likely different processes
1976    to follow for securing recurring funds, as compared with requesting one-time funding.  For
1977    example, funding for a new information system to support a C-SCRM capability may involve the

1978    development of a formal business case that must be presented to an organization's investment
1979    review board for approval. Breaking out resource needs into ongoing and one-time costs, as well
1980    as into cost categories that align with budget formulation, resource decision-making, and the
1981    allocation and management of available funds will also be helpful.
1982
1983    It is recommended that the C-SCRM PMO have the lead responsibility of coordinating with
1984    mission/business process and budget officials to build out and maintain a multi-year C-SCRM
1985    program budget that captures both recurring and non-recurring resource requirements and maps
1986    those requirements to available funding and fund sources. To understand what amount of funding
1987    is required, at what time, and for what purpose, organizations should identify and assess which
1988    type and level of resources (people or things), are required to implement a C-SCRM program
1989    capability and perform required C-SCRM processes on an ongoing basis.  The costs associated
1990    with each of these identified resource needs would then be captured, accumulated, and reflected
1991    in a budget that includes line items for relevant cost categories, such as personnel costs,
1992    contracts, training, travel, or tools and systems. This will provide the organization a baseline
1993    understanding of what can be accomplished within existing resource levels and where there are
1994    gaps in need of being filled. The actual allocation of funds may be centralized in a single C-
1995    SCRM budget or may be dispersed across the organization and reflected in individual office or
1996    mission/business process-area budgets.  Regardless of how funds are actually assigned, having a
1997    centralized picture of the C-SCRM budget and funds status will serve as a valuable source of
1998    information that justify new requests, inform prioritization decisions and adjust expectations
1999    about certain activities and the duration in which they can be accomplished.
2000
2001    Ensuring C-SCRM program funding is distinctly identified within the organization's budget—
2002    with performance measures linked to the funding—will drive accountability for results. The
2003    visible dedication of funds in budget requests and performance plans and reports compels
2004    leadership attention on C-SCRM processes and accomplishment of objectives.  Budgets must be
2005    requested and justified on a periodic basis and this process allows leadership and oversight
2006    officials to trace and measure the effectiveness and efficiency of allocated resources.  This, in
2007    turn, serves as a driving function for program and operational C-SCRM personnel to track and
2008    manage their performance.

2009

2010 **4.  C-SCRM CONTROLS**

2011 NIST defines security controls as:

2012
2013        *The management, operational, and technical controls (i.e., safeguards or*
2014        *countermeasures) prescribed for an information system to protect the*
2015        *confidentiality, integrity, and availability of the system and its information. [FIPS*
2016        *200, FIPS 199, CNSSI No. 4009, NIST SP 800-37 Rev. 1, NIST SP 800-53 Rev. 5,*
2017        *NIST SP 800-53A Rev. 5]*
2018
2019 NIST SP 800-53 Rev. 5 defines numerous cyber supply chain-related controls within the catalog
2020 of information security controls. This section is structured as an enhanced overlay of NIST SP
2021 800-53 Rev. 5. It identifies and augments C-SCRM-related controls with additional supplemental
2022 guidance and provides new controls as appropriate. The C-SCRM controls are organized into the
2023 twenty (20) control families of NIST SP 800-53 Rev. 5. This approach facilitates use of the
2024 security controls assessment techniques provided in NIST SP 800-53A Rev. 5 to assess
2025 implementation of C-SCRM controls.
2026
2027 The controls provided in this publication are intended for organizations to implement internally,
2028 as well as require of their contractors and subcontractors, if and when applicable, and as
2029 incorporated into a contractual agreement. As with NIST SP 800-53 Rev. 5, the security controls
2030 and control enhancements are a starting point from which controls/enhancements may be
2031 removed, added, or specialized based on an organization's needs. Each control in this section is
2032 listed for its applicability to C-SCRM. Those controls from NIST SP 800-53 Rev. 5 not listed are
2033 not considered directly applicable to C-SCRM, and thus are not included in this publication.
2034 Details and supplemental guidance for the various C-SCRM controls in this publication are
2035 contained in Section 4.5.
2036
2037 **4.1  C-SCRM CONTROLS SUMMARY**
2038
2039 During the Respond Step of the risk management process discussed in Section 2, organizations
2040 select, tailor, and implement controls for mitigating cyber supply chain risk. NIST 800-53B lists
2041 a set of information security controls at the FIPS 199 high-, moderate-, and low-impact levels.
2042 This section describes how these controls help mitigate risk to information systems and
2043 components, as well as the cyber supply chain infrastructure. The section provides twenty (20)
2044 C-SCRM control families that include relevant controls and supplemental guidance.
2045
2046 Figure 4-1 depicts the process used to identify, refine, and add C-SCRM supplemental guidance
2047 to the NIST SP 800-53 Rev. 5 C-SCRM-related controls. The figure, which repeats Figure 1-5,
2048 represents the following steps:
2049
2050    1.  Selected and extracted individual controls and enhancements from NIST SP 800-53 Rev.
2051        5 that were applicable to C-SCRM;
2052    2.  Analyzed these controls to determine how they apply to C-SCRM;
2053    3.  Evaluated the resulting set of controls and enhancements to determine whether all C-
2054        SCRM concerns were addressed;
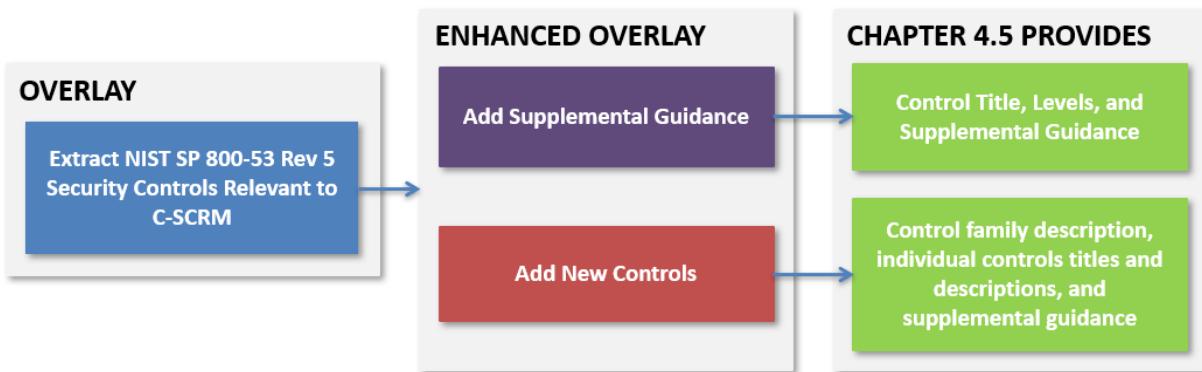
2055    4.  Developed additional controls currently not defined in NIST SP 800-53 Rev. 5;
2056    5.  Identified controls for flow down to relevant sub-level contractors;
2057    6.  Assigned applicable levels to each C-SCRM control; and
2058    7.  Developed C-SCRM-specific supplemental guidance for each C-SCRM control.
2059
2060



2061
2062
2063       **Fig. 4-1: C-SCRM Security Controls in NIST SP 800-161 Revision 1, Section 4.5**

2064
2065    Note that NIST SP 800-53 Rev. 5 provides C-SCRM-related controls and control families. These
2066    controls may be listed in this publication with a summary or additional guidance and a reference
2067    to the original NIST SP 800-53 Rev. 5 control and supplemental guidance detail.
2068
2069    **4.2   C-SCRM CONTROLS THROUGHOUT THE ORGANIZATION**
2070
2071    As noted in Table 4-1, C-SCRM controls in this publication are designated by the three levels
2072    comprising the organization. This is to facilitate C-SCRM control selection specific to
2073    organizations, their various missions, and individual systems, as described in Appendix C under
2074    the Respond step of the risk management process. During controls selection, organizations
2075    should use the C-SCRM controls in this section to identify appropriate C-SCRM controls for
2076    tailoring, per risk assessment. By selecting and implementing applicable C-SCRM controls for
2077    each level, organizations will ensure that they have appropriately addressed C-SCRM throughout
2078    their organizations.
2079
2080    **4.3   APPLYING C-SCRM CONTROLS TO ACQUIRING PRODUCTS AND SERVICES**
2081
2082    Acquirers may use C-SCRM controls as the basis from which to communicate their C-SCRM
2083    requirements to different types of organizations, described within this publication, that provide
2084    products and services to acquirers, including suppliers, developers, system integrators, external
2085    system service providers, and other ICT/OT-related service providers. Acquirers should avoid
2086    using generalized requirements statements, such as "ensure compliance with NIST SP 800-161
2087    Rev. 1 controls." Acquirers must be careful to select the controls relevant to the specific use case
2088    of the service or product being acquired.  Acquirers are encouraged to integrate C-SCRM

2089    throughout their acquisition activities. More details on the role of C-SCRM in acquisition is
2090    provided in Section 3.1 of this document.
2091
2092    It is important to recognize the controls in this section do not provide specific contracting
2093    language. Acquirers should develop their own contracting language using this publication as
2094    guidance to develop specific C-SCRM requirements for inclusion in contracts. The following
2095    sections expand upon the supplier, developer, system integrator, external system service
2096    provider, and other ICT/OT-related service provider roles with respect to C-SCRM expectations
2097    for acquirers.
2098
2099    Organizations may use multiple techniques to ascertain w these controls are in place. Techniques
2100    may include supplier self-assessment, acquirer review, or third-party assessments for
2101    measurement and conformance to the organization's requirements. Organizations should first
2102    look to established third-party assessments to see if they meet their needs. When an organization
2103    defines C-SCRM requirements, it may discover that established third-party assessments may not
2104    address all specific requirements. In this case, additional evidence may be needed to justify
2105    additional requirements. Please note that the data obtained for this purpose should be
2106    appropriately protected.
2107
2108    ### 4.3.1    Suppliers

2109    Suppliers may provide either commercial off-the-shelf (COTS) or, in federal contexts,
2110    government off-the-shelf (GOTS) solutions to the acquirer. COTS solutions include non-
2111    developmental items (NDI), such as commercially licensing solutions/products, which include
2112    Open Source Solutions (OSS). GOTS solutions are government-only license-able solutions.
2113    Suppliers are a diverse group, ranging from very small to large, specialized to diversified, based
2114    in a single country to transnational, and range widely in the level of sophistication, resources,
2115    and transparency/visibility in both process and solution.
2116
2117    Suppliers also have diverse levels and types of C-SCRM practices in place. These practices and
2118    other related practices may provide the evidence needed for SCRM evaluation. An example of a
2119    federal resource that may be leveraged is the Defense Microelectronics Activity (DMEA)
2120    accreditation for Trusted Suppliers. When appropriate, allow suppliers the opportunity to reuse
2121    any existing data and documentation that may provide evidence of C-SCRM implementation.
2122
2123    Organizations should consider whether the cost of doing business with suppliers may be directly
2124    impacted by the extent of cyber supply chain requirements imposed on suppliers, the willingness
2125    or ability of suppliers to allow visibility into how their products are developed or manufactured
2126    and how they apply security and supply chain practices to their solutions. When organizations or
2127    system integrators require greater levels of transparency from suppliers, they must consider the
2128    possible cost implications of such requirements. Suppliers may opt not to participate in
2129    procurements to avoid increased costs or perceived risks to their intellectual property, limiting an
2130    organization's supply or technology choices. Additionally, suppliers may face risk from
2131    customers imposing multiple, different sets of cyber supply chain requirements with which the
2132    supplier must comply on a per-customer basis.
2133

2134   *4.3.2   Developers*

2135   Developers are personnel that develop or manufacture systems, system components (e.g.,
2136   software) or system services (e.g., Application Programming Interfaces (APIs)). Development
2137   can occur internally within organizations or through external entities. Developers typically
2138   maintain privileged access rights and play an essential role throughout the SDLC. The activities
2139   they perform and the work they produce can either enhance security or introduce new
2140   vulnerabilities. It is therefore essential that developers are both subject to, and intimately familiar
2141   with, C-SCRM requirements and controls.
2142
2143   *4.3.3   System Integrators*

2144   System integrators are those entities which provide customized services to the acquirer including
2145   custom development, test, operations, and maintenance. This group usually replies to a request
2146   for proposal from an acquirer with a proposal describing a solution or service that is customized
2147   to the acquirer's requirements. Such proposals provided by system integrators can include many
2148   layers of suppliers and may include teaming arrangements with other vendors or subcontractors.
2149   The system integrator should ensure these business entities are vetted and verified with respect to
2150   the acquirer's C-SCRM requirements. Because of the level of visibility that can be obtained in
2151   the relationship with the system integrator, the acquirer has the discretion to require rigorous
2152   supplier acceptance criteria as well as any relevant countermeasures to address identified or
2153   potential risks.
2154
2155   *4.3.4   External System Service Providers of Information System Services*

2156   Organizations use external service providers to perform or support some of their mission and
2157   business functions (NIST SP 800-53 Rev. 5). The outsourcing of systems and services creates a
2158   set of cyber supply chain concerns that reduces the acquirer's visibility into, and control of, the
2159   outsourced functions. Therefore, it requires increased rigor from organizations in defining C-
2160   SCRM requirements, stating them in procurement agreements, and then monitoring delivered
2161   services and evaluating them for compliance with the stated requirements. Regardless of who
2162   performs the services, the acquirer is ultimately responsible and accountable for the risk to the
2163   organization's systems and data that may result from using these services. Organizations should
2164   implement a set of compensating C-SCRM controls to address this risk and work with the
2165   mission/business process owner or risk executive to accept this risk. A variety of methods may
2166   be used to communicate and subsequently verify and monitor C-SCRM requirements through
2167   such vehicles as contracts, interagency agreements, lines of business arrangements, licensing
2168   agreements, and/or supply chain transactions.
2169
2170   *4.3.5   Other ICT/OT-related Service Providers*

2171   Providers of services can perform a wide range of different functions ranging from consulting to
2172   posting content on a website to janitorial services. Other ICT/OT-related Service Providers
2173   encompass those providers that require physical or logical access to ICT/OT or use technology
2174   (e.g., an aerial photographer using a drone to take video/pictures or a security firm remotely
2175   monitoring a facility using cloud-based video surveillance) as a means to deliver their service.
2176   As a result of service provider access or use, there is the potential for cyber-supply chain risk to
2177   be introduced to the organization.
2178

2179    Operational technology possesses unique operational and security characteristics that demand
2180    specialized skills and capabilities to effectively protect them. Organizations that have significant
2181    OT components throughout their enterprise architecture therefore often turn to specialized
2182    service providers for secure implementation and maintenance of these devices, systems, or
2183    equipment. Any organization or individual providing services which may include authorized
2184    access to an ICT or OT system should adhere to organizational C-SCRM requirements. Scrutiny
2185    should be paid particularly to ICT/OT-related service providers managing mission critical and/or
2186    safety-relevant assets.
2187
2188    **4.4  SELECTING AND TAILORING IMPLEMENTING C-SCRM SECURITY**
2189        **CONTROLS**
2190
2191    The C-SCRM controls defined in this section should be selected and tailored according to
2192    individual organization needs and environment using the guidance in NIST SP 800-53 Rev. 5, in
2193    order to ensure a cost-effective, risk-based approach to providing C-SCRM organization-wide.
2194    The C-SCRM baseline defined in this publication addresses the basic needs of a broad and
2195    diverse set of constituencies. Organizations must select, tailor, and implement the security
2196    controls based on: (i) the environments in which organizational information systems are acquired
2197    and operate; (ii) the nature of operations conducted by organizations; (iii) the types of threats
2198    facing organizations, missions/business processes, supply chains, and information systems; and
2199    (iv) the type of information processed, stored, or transmitted by information systems and the
2200    supply chain infrastructure.
2201
2202    After selecting the initial set of security controls, the acquirer should initiate the tailoring process
2203    according to NIST SP 800-53B *Control Baselines for Information Systems and Organization* in
2204    order to appropriately modify and more closely align the selected controls with the specific
2205    conditions within the organization. The tailoring should be coordinated with and approved by the
2206    appropriate organizational officials (e.g., authorizing officials, authorizing official designated
2207    representatives, risk executive (function), chief information officers, or senior information
2208    security officers) prior to implementing the C-SCRM controls. Additionally, organizations have
2209    the flexibility to perform the tailoring process at the enterprise level (either as the required
2210    tailored baseline or as the starting point for policy, program or system-specific tailoring), in
2211    support of a specific program at the individual information system level, or using a combination
2212    of enterprise-level, program/mission-level and system-specific approaches.
2213
2214    Selection and tailoring decisions, including the specific rationale for those decisions, should be
2215    included within the C-SCRM documentation at Levels 1, 2, and 3 and Appendix C and approved
2216    by the appropriate organizational officials as part of the C-SCRM Plan approval process.
2217
2218    *4.4.1    C-SCRM Control Format*
2219
2220    Table 4-2 shows the format used in this publication for controls which provide supplemental C-
2221    SCRM guidance on existing NIST SP 800-53 Rev. 5 controls or control enhancements.
2222
2223    C-SCRM controls that do not have a parent NIST SP 800-53 Rev. 5 control generally follow the
2224    format described in NIST SP 800-53 Rev. 5, with the addition of relevant levels. New controls

2225  are given identifiers consistent with NIST SP 800-53 Rev. 5, but do not duplicate existing
2226  control identifiers.
2227
2228                          **Table 4-1: C-SCRM Control Format**

| CONTROL IDENTIFIER | CONTROL NAME |
|---|---|
| | Supplemental C-SCRM Guidance: |
| | Level(s): |
| | Related Control(s): |
| | Control Enhancement(s): |
| **(1)** | *CONTROL NAME | CONTROL ENHANCEMENT NAME* |
| | Supplemental C-SCRM Guidance: |
| | Level(s): |
| | Related Control(s): |

2229

2230  An example of the C-SCRM control format is shown below using C-SCRM Control AC-3 and
2231  SCRM Control Enhancement AC-3(8):

2232  **AC-3    ACCESS ENFORCEMENT**

2233       Supplemental C-SCRM Guidance: Ensure that the information systems and the supply chain have
2234       appropriate access enforcement mechanisms in place. This includes both physical and logical access
2235       enforcement mechanisms, which likely work in coordination for supply chain needs. Organizations should
2236       ensure a detailed definition of access enforcement.
2237
2238       Level(s): 2, 3
2239
2240       Related Control(s): AC-4
2241
2242       Control Enhancement(s):

2243       *(8)   ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS*

2244       **(1)**  Supplemental C-SCRM Guidance: Prompt revocation is critical to ensure that suppliers, developers,
2245             system integrators, external system service providers, and other ICT/OT-related service providers who
2246             no longer require access, or who abuse or violate their access privilege, are not able to access an
2247             organization's system. For example, in a "badge flipping" situation, a contract is transferred from one
2248             system integrator organization to another with the same personnel supporting the contract. In that
2249             situation, the organization should disable the existing accounts, retire the old credentials, establish new
2250             accounts, and issue completely new credentials.
2251
2252             Level(s): 2, 3
2253

*4.4.2    Using C-SCRM Controls in this Publication*

The remainder of Section 4 provides the enhanced C-SCRM overlay of NIST SP 800-53 Rev. 5. This section displays the relationship between NIST SP 800-53 Revision 5 controls and C-SCRM controls in one of the following ways:

- If a NIST SP 800-53 Rev. 5 control or enhancement was determined to be an information security control that serves as a foundational control for C-SCRM, but is not specific to C-SCRM, it is not included in this publication.
- If a NIST SP 800-53 Rev. 5 control or enhancement was determined to be relevant to C-SCRM, the levels in which the control applies are also provided.
- If a NIST SP 800-53 Rev.5 enhancement was determined to be relevant to C-SCRM, but the parent control was not, the parent control number and title is included, but there is no supplemental C-SCRM guidance.
- C-SCRM controls/enhancements that do not have an associated NIST 800-53 Rev. 5 control/enhancement are listed with their titles and the control/enhancement text.
- All C-SCRM controls include the levels in which the control applies and supplemental C-SCRM guidance as applicable.
- When a control enhancement provides a mechanism for implementing the C-SCRM control, the control enhancement is listed within the Supplemental C-SCRM Guidance and is not included separately.
- If NIST SP 800-53 Rev. 5 already captures withdrawals or reorganization of prior NIST SP 800-161 controls, it is not included.

The following new controls and control enhancement have been added:

- The C-SCRM Control MA-8 – Maintenance Monitoring and Information Sharing is added to the Maintenance control family; and
- The C-SCRM Control SR-13 – Supplier Inventory is added to the Supply Chain Risk Management control family.

## 4.5  C-SCRM SECURITY CONTROLS

**FAMILY: ACCESS CONTROL**

FIPS 200 specifies the Access Control minimum security requirement as follows:

> *Organizations must limit information system access to authorized users, processes*
> *acting on behalf of authorized users, or devices (including other information systems)*
> *and to the types of transactions and functions that authorized users are permitted to*
> *exercise.*

Systems and components that traverse the supply chain are subject to access by a variety of individuals and organizations, including suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Such access should be defined and managed to ensure that it does not inadvertently result in unauthorized release, modification, or destruction of information. This access should be limited to only the necessary type, duration, and level of access for authorized organizations (and authorized individuals within those organizations) and monitored for cyber supply chain impact.

**AC-1    POLICY AND PROCEDURES**

Supplemental C-SCRM Guidance: Organizations should specify and include in agreements (e.g., contracting language) access control policies for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. These should include both physical and logical access to the cyber supply chain and the information system. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 1, 2, 3

**AC-2    ACCOUNT MANAGEMENT**

Supplemental C-SCRM Guidance: Use of this control helps establish traceability of actions and actors in the cyber supply chain. This control also helps ensure access authorizations of actors in the supply chain is appropriate on a continuous basis. The organization may choose to define a set of roles and associate a level of authorization to ensure proper implementation. Organizations must ensure that accounts for contractor personnel do not exceed the period of performance of the contract. Privileged accounts should only be established for appropriately vetted contractor personnel. Organizations should also have processes in place to establish and manage temporary or emergency accounts for contractor personnel that require access to a mission-critical or mission-enabling system during a continuity or emergency event. For example, during a pandemic event, existing contractor personnel who are not able to work due to illness may need to be temporarily backfilled by new contractor staff.

Level(s): 2, 3

**AC-3    ACCESS ENFORCEMENT**

Supplemental C-SCRM Guidance: Ensure that the information systems and the supply chain have appropriate access enforcement mechanisms in place. This includes both physical and logical access enforcement mechanisms, which likely work in coordination for supply chain needs. Organizations should ensure a defined consequence framework is in place to address access control violations.

Level(s): 2, 3

Control Enhancement(s):

**(8)** *ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS*

Supplemental C-SCRM Guidance: Prompt revocation is critical to ensure that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers who no longer require access, or who abuse or violate their access privilege, are not able to access an organization's system. Organizations should include in their agreements a requirement for contractors, and sub-tier contractors, to immediately return access credentials (e.g., tokens, PIV or CAC cards, etc.) to the organization and organizations must have processes in place to promptly process the revocation of access authorizations. For example, in a "badge flipping" situation, a contract is transferred from one system integrator organization to another with the same personnel supporting the contract. In that situation, the organization should disable the existing accounts, retire the old credentials, establish new accounts, and issue completely new credentials.

Level(s): 2, 3

**(9)** *ACCESS ENFORCEMENT | CONTROLLED RELEASE*

Supplemental C-SCRM Guidance: Information about the cyber supply chain should be controlled for release between the organization and third parties. Information may be exchanged between the organization and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Controlled release of organizational information provides protection to manage risks associated with disclosure.

Level(s): 2, 3

## AC-4    INFORMATION FLOW ENFORCEMENT

Supplemental C- SCRM Guidance: Supply chain information may traverse a large cyber supply chain to a broad set of stakeholders including the organization and its various federal stakeholders, as well as suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Specifying the requirements as well as how information flow is enforced should ensure that only the required information, and not more, is communicated to the various participants in the cyber supply chain. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

Control Enhancement(s):

**(6)** *INFORMATION FLOW ENFORCEMENT | METADATA*

Supplemental C-SCRM Guidance: Metadata relevant to C-SCRM is quite extensive and includes activities within the SDLC. For example, information about systems and system components, acquisition details, and delivery is considered metadata and may require appropriate protections. Organizations should identify what metadata is directly relevant to their supply chain security and ensure that information flow enforcement is implemented in order to protect applicable metadata.

Level(s): 2, 3

**(17)** *INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION*

2374     Supplemental C-SCRM Guidance: Within the C-SCRM context, organizations should specify various
2375     source and destination points for information about the cyber supply chain and information that flows
2376     through the cyber supply chain. This is so that organizations have visibility of information flow within
2377     the cyber supply chain.

2378
2379     Level(s): 2, 3

2380     **(19)** *INFORMATION FLOW ENFORCEMENT | VALIDATION OF METADATA*

2381     Supplemental C-SCRM Guidance: For C-SCRM, validation of data and the relationship to its metadata
2382     are critical. Much of the data transmitted through the cyber supply chain is validated with the
2383     verification of the associated metadata that is bound to it. Ensure that proper filtering and inspection is
2384     put in place for validation before allowing payloads into the cyber supply chain.

2385
2386     Level(s): 2, 3

2387     **(21)** *INFORMATION FLOW ENFORCEMENT | PHYSICAL OR LOGICAL SEPARATION OF INFORMATION*
2388     *FLOWS*

2389     Supplemental C-SCRM Guidance: The organization should ensure the separation of the information
2390     system and cyber supply chain information flow. Various mechanisms can be implemented including,
2391     for example, encryption methods (e.g., digital signing). Addressing information flow between the
2392     organization and its suppliers, developers, system integrators, external system service providers, and
2393     other ICT/OT-related service providers may be challenging, especially when leveraging public
2394     networks.

2395
2396     Level(s): 3

2397   **AC-5**   **SEPARATION OF DUTIES**

2398     Supplemental C-SCRM Guidance: The organization should ensure that appropriate separation of duties is
2399     established for decisions requiring the acquisition of both information system and cyber supply chain
2400     components. Separation of duties helps to ensure that adequate protections are in place for components
2401     entering the organization's cyber supply chain. An example may be developers not having privileges to
2402     promote code they wrote from development to production environments.

2403     Level(s): 2, 3

2404   **AC-6**   **LEAST PRIVILEGE**

2405     Supplemental C-SCRM Guidance: For C-SCRM supplemental guidance, see control enhancements.
2406

2407     Control Enhancement(s):

2408     **(6)** *LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*

2409     Supplemental C-SCRM Guidance: Organizations should ensure that protections are in place to prevent
2410     non-organizational users from having privileged access to organizational cyber supply chain and
2411     related supply chain information. When organizational users may include independent consultants,
2412     suppliers, developers, system integrators, external system service providers, and other ICT/OT-related
2413     service providers, relevant access requirements may need to be more precisely defined regarding which
2414     information and/or components are accessible, for what duration, at which frequency, using which
2415     access methods, and by whom, using least privilege mechanisms. Understanding which components
2416     are critical and noncritical can aid in understanding the level of detail that may need to be defined
2417     regarding least privilege access for non-organizational users.
2418

2419        Level(s): 2, 3

2420    **AC-17   REMOTE ACCESS**

2421        Supplemental C-SCRM Guidance: Evermore frequently, cyber supply chains are accessed remotely.
2422        Whether for the purpose of development, maintenance, or operation of information systems, organizations
2423        should implement secure remote access mechanisms and allow remote access only to vetted personnel.
2424        Remote access to an organization's cyber supply chain (including distributed software development
2425        environments) should be limited to the organization or contractor personnel and only if and as required to
2426        perform their tasks. Remote access requirements, such as a requirement to use a secure VPN, employ multi-
2427        factor authentication, limit access to specified business hours, or from specified geographic locations, must
2428        be properly defined in agreements. Organizations should require its prime contractors to implement this
2429        control and flow down this requirement to relevant sub-tier contractors.

2430        Level(s): 2, 3

2431        Control Enhancement(s):

2432        **(6)**  *REMOTE ACCESS | PROTECTION OF MECHANISM INFORMATION*

2433            Supplemental C-SCRM Guidance: Organizations should ensure that detailed requirements are properly
2434            defined and access to information regarding the information system and cyber supply chain is
2435            protected from unauthorized use and disclosure. Since cyber supply chain data and metadata disclosure
2436            or access can have significant implications to an organization's mission processes, appropriate
2437            measures must be taken to vet both the cyber supply chain and personnel processes to ensure that
2438            adequate protections are implemented. Ensure that remote access to such information is included in
2439            requirements.
2440
2441            Level(s): 2, 3

2442    **AC-18   WIRELESS ACCESS**

2443        Supplemental C-SCRM Guidance: An organization's cyber supply chain may include wireless
2444        infrastructure that supports supply chain logistics (e.g., Radio Frequency Identification Device (RFID)
2445        support, software call home features). Supply chain systems/components traverse the cyber supply chain as
2446        they are moved from one location to another, whether within the organization's own environment or during
2447        delivery from system integrators or suppliers. Ensuring appropriate access mechanisms are in place within
2448        this cyber supply chain enables the protection of the information systems and components, as well as
2449        logistics technologies and metadata used during shipping (e.g., within tracking sensors). The organization
2450        should explicitly define appropriate wireless access control mechanisms for the cyber supply chain in
2451        policy and implement appropriate mechanisms.

2452        Level(s): 1, 2, 3

2453    **AC-19   ACCESS CONTROL FOR MOBILE DEVICES**

2454        Supplemental C-SCRM Guidance: Use of mobile devices (e.g., laptops, tablets, e-readers, smartphones,
2455        smartwatches) has become common in the cyber supply chain. They are used in direct support of an
2456        organization's operations as well as for purposes such as tracking supply chain logistics data as information
2457        systems and components traverse organization or systems integrator supply chains. Ensure that access
2458        control mechanisms are clearly defined and implemented where relevant when managing organizations
2459        cyber supply chain components. An example of such an implementation includes access control
2460        mechanisms implemented for use with remote handheld units in RFID for tracking components that

2461 traverse the supply chain. Access control mechanisms should also be implemented on any associated data
2462 and metadata tied to the devices.

2463 Level(s): 2, 3

2464 **AC-20   USE OF EXTERNAL SYSTEMS**

2465 Supplemental C-SCRM Guidance: Organizations' external information systems include those of suppliers,
2466 developers, system integrators, external system service providers, and other ICT/OT-related service
2467 providers. Unlike in an acquirer's internal organization where direct and continuous monitoring is possible,
2468 in the external supplier relationship, information may be shared on an as-needed basis and should be
2469 articulated in an agreement. Access to the cyber supply chain from such external information systems
2470 should be monitored and audited. Organizations should require its prime contractors to implement this
2471 control and flow down this requirement to relevant sub-tier contractors.

2472 Level(s): 1, 2, 3

2473 Control Enhancement(s):

2474 **(1)**   *USE OF EXTERNAL SYSTEMS | LIMITS ON AUTHORIZED USE*

2475 Supplemental C-SCRM Guidance: This enhancement helps limit exposure of the cyber supply chain to
2476 the suppliers', developers', system integrators', external system service providers', and other ICT/OT-
2477 related service providers' systems.

2478 Level(s): 2, 3

2479 **(3)**   *USE OF EXTERNAL SYSTEMS | NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE*
2480
2481 Supplemental C-SCRM Guidance: Devices that do not belong to the organization (e.g., bring your own
2482 device (BYOD) policies) increase the organization's exposure to cyber supply chain risks. This
2483 includes devices used by suppliers, developers, system integrators, external system service providers,
2484 and other ICT/OT-related service providers. Organizations should review the use of non-organization
2485 devices by non-organization personnel and make a risk-based decision as to whether it will allow use
2486 of such devices or furnish devices. Organizations should furnish devices to those non-organization
2487 personnel that present unacceptable cyber supply chain risk.
2488
2489 Level(s): 2, 3

2490 **AC-21   INFORMATION SHARING**

2491 Supplemental C-SCRM Guidance: Sharing information within the cyber supply chain can help to manage
2492 cyber supply chain risks. This information may include vulnerabilities, threats, criticality of systems and
2493 components, or delivery information. This information sharing should be carefully managed to ensure that
2494 the information is accessible only to authorized individuals within the organization's cyber supply chain.
2495 Organizations should clearly define boundaries for information sharing with respect to temporal,
2496 informational, contractual, security, access, system, and other requirements. Organizations should monitor
2497 and review for unintentional or intentional information sharing within its cyber supply chain activities
2498 including information sharing with suppliers, developers, system integrators, external system service
2499 providers, and other ICT/OT-related service providers.

2500 Level(s): 1, 2

2501 **AC-22   PUBLICLY ACCESSIBLE CONTENT**

2502    Supplemental C-SCRM Guidance: Within the C-SCRM context, publicly accessible content may include
2503    Requests for Information, Requests for Proposal, or information about delivery of systems and components.
2504    This information should be reviewed to ensure that only appropriate content is released for public
2505    consumption, alone or in aggregation with other information.

2506    Level(s): 2, 3

2507  **AC-23   DATA MINING PROTECTION**

2508    Supplemental C-SCRM Guidance: Organizations should require its prime contractors to implement this
2509    control as part of their insider threat activities and flow down this requirement to relevant sub-tier
2510    contractors.

2511    Level(s): 2, 3

2512  **AC-24   ACCESS CONTROL DECISIONS**

2513    Supplemental C-SCRM Guidance: Organizations should assign access control decisions to support
2514    authorized accesses to the cyber supply chain. Ensure that if a system integrator or external service provider
2515    is used, there is consistency in access control decision requirements and how the requirements are
2516    implemented to deliver consistency in support of the organization's supply chain needs. This may require
2517    defining such requirements in service-level agreements in many cases as part of the upfront relationship
2518    established between the organization and system integrator or the organization and external service
2519    provider. Organizations should require its prime contractors to implement this control and flow down this
2520    requirement to relevant sub-tier contractors.

2521    Level(s): 1, 2, 3
2522

2523    **FAMILY: AWARENESS AND TRAINING**
2524
2525    FIPS 200 specifies the Awareness and Training minimum security requirement as follows:
2526
2527        *Organizations must: (i) ensure that managers and users of organizational information*
2528        *systems are made aware of the security risks associated with their activities and of the*
2529        *applicable laws, Executive Orders, directives, policies, standards, instructions,*
2530        *regulations, or procedures related to the security of organizational information*
2531        *systems; and (ii) ensure that organizational personnel are adequately trained to carry*
2532        *out their assigned information security-related duties and responsibilities.*
2533
2534    NIST SP 800-161 Rev. 1 expands the Awareness and Training control of FIPS 200 to include C-
2535    SCRM. Making the workforce aware of C-SCRM concerns is key to a successful C-SCRM
2536    strategy. C-SCRM awareness and training provides understanding of the problem space and of
2537    the appropriate processes and controls that can help mitigate cyber supply chain risk.
2538    Organizations should provide C-SCRM awareness and training to individuals at all levels within
2539    the organization including, for example, information security, procurement, enterprise risk
2540    management, engineering, software development, IT, legal, HR, and others. Organizations
2541    should also work with suppliers, developers, system integrators, external system service
2542    providers, and other ICT/OT-related service providers to ensure the personnel that interact with
2543    an organization's cyber supply chains receive C-SCRM awareness and training, as appropriate.
2544

2545    **AT-1    POLICY AND PROCEDURES**

2546        Supplemental C-SCRM Guidance: Organizations should designate a specific official to manage the
2547        development, documentation, and dissemination of the awareness and training policy and procedures that
2548        includes C-SCRM as well as role-based specific training for those with supply chain responsibilities.
2549        Organizations should integrate cyber supply chain risk management training and awareness into the
2550        security training and awareness policy. The C-SCRM training should target both the organization and its
2551        contractors. The policy should ensure that cyber supply chain role-based training is required for those
2552        individuals or functions that touch or impact the cyber supply chain, such as information system owner,
2553        acquisition, supply chain logistics, system engineering, program management, IT, quality, and incident
2554        response.
2555
2556        C-SCRM training procedures should address:
2557            a.  Roles throughout the cyber supply chain and system/element life cycle to limit opportunities and
2558                means available to individuals performing these roles that could result in adverse consequences;
2559            b.  Requirements for interaction between an organization's personnel and individuals not employed
2560                by the organization that participate in the cyber supply chain throughout the SDLC; and
2561            c.  Incorporating feedback and lessons learned from C-SCRM activities into the C-SCRM training.

2562        Level(s): 1, 2

2563    **AT-2    LITERACY TRAINING AND AWARENESS**

2564        Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance provided in control
2565        enhancements.

2566        Control Enhancements:

2567     **(1)** *LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES*

2568        Supplemental C-SCRM Guidance: Organizations should provide practical exercises in literacy training
2569        that simulate cyber supply chain events and incidents. Organizations should require its prime
2570        contractors to implement this control and flow down this requirement to relevant sub-level contractors

2571     **(2)** *LITERACY TRAINING AND AWARENESS | INSIDER THREAT*

2572        Supplemental C-SCRM Guidance: Organizations should provide literacy training on recognizing and
2573        reporting potential indicators of insider threat within the cyber supply chain. Organizations should
2574        require its prime contractors to implement this control and flow down this requirement to relevant sub-
2575        tier contractors.

2576     **(3)** *LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING*

2577        Supplemental C-SCRM Guidance: Organizations should provide literacy training on recognizing and
2578        reporting potential and actual instance of cyber supply chain related social engineering and social
2579        mining. Organizations should require its prime contractors to implement this control and flow down
2580        this requirement to relevant sub-level contractors

2581     **(4)** *LITERACY TRAINING AND AWARENESS | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS*
2582          *SYSTEM BEHAVIOR*

2583        Supplemental C-SCRM Guidance: Provide literacy training on recognizing suspicious communications
2584        on anomalous behavior in organizational supply chain systems. Organizations should require its prime
2585        contractors to implement this control and flow down this requirement to relevant sub-level contractors.

2586     **(5)** *LITERACY TRAINING AND AWARENESS | ADVANCED PERSISTENT THREAT*

2587        Supplemental C-SCRM Guidance: Provide literacy training on recognizing suspicious communications
2588        on advanced persistent threat (APT) in the organization's cyber supply chain. Organizations should
2589        require its prime contractors to implement this control and flow down this requirement to relevant sub-
2590        level contractors

2591     **(6)** *LITERACY TRAINING AND AWARENESS | CYBER THREAT ENVIRONMENT*

2592        Supplemental C-SCRM Guidance: Provide literacy training on cyber threats specific to the
2593        organization's supply chain environment. Organizations should require its prime contractors to
2594        implement this control and flow down this requirement to relevant sub-level contractors

2595     Level(s): 2

2596   **AT-3**   **ROLE-BASED TRAINING**

2597     Supplemental C-SCRM Guidance: Addressing cyber-supply chain risks throughout the acquisition process
2598     is essential to performing C-SCRM effectively. Personnel who are part of the acquisition workforce require
2599     training on what C-SCRM requirements, clauses, and evaluation factors are necessary to include when
2600     conducting a procurement and how to incorporate C-SCRM into each acquisition phase. Similar enhanced
2601     training requirements should be tailored for personnel responsible for conducting threat assessments and
2602     involved in responding to threats and identified risks require training in counter-intelligence awareness and
2603     reporting.

2604     Control Enhancement(s):

2605     **(7)** *SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*

Supplemental C-SCRM Guidance: C-SCRM is impacted by a number of physical security mechanisms and procedures within the supply chain, such as manufacturing, shipping, and receiving, physical access to facilities, inventory management, and warehousing. Organization and system integrator personnel providing development and operational support to the organization should receive training on how to handle these physical security mechanisms and on the associated cyber supply chain risks.

Level(s): 2

**(6)** *ROLE-BASED TRAINING | COUNTERINTELLIGENCE TRAINING*

Supplemental C-SCRM Guidance: Public sector organizations should provide specialized counterintelligence awareness training that enables its resources to collect, interpret, and act upon a range of data sources that may signal the presence of a foreign adversary's presence in the cyber supply chain. Counterintelligence training should at a minimum cover known red flags, key information sharing concepts, and reporting requirements.

Level(s): 2

**AT-4    TRAINING RECORDS**

Supplemental C-SCRM Guidance: Organizations should maintain documentation for C-SCRM-specific training, especially in regard to key personnel in acquisitions and counterintelligence.

Level(s): 2

2626 **FAMILY: AUDIT AND ACCOUNTABILITY**
2627
2628 FIPS 200 specifies the Audit and Accountability minimum security requirement as follows:
2629
2630     *Organizations must: (i) create, protect, and retain information system audit records to*
2631     *the extent needed to enable the monitoring, analysis, investigation, and reporting of*
2632     *unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure*
2633     *that the actions of individual information system users can be uniquely traced to those*
2634     *users so they can be held accountable for their actions.*
2635
2636 Audit and accountability controls for C-SCRM provide information useful in the event of a cyber
2637 supply chain incident or compromise. Organizations should ensure they designate and audit
2638 cyber supply chain-relevant events within their information system boundaries using appropriate
2639 audit mechanisms (e.g., system logs, Intrusion Detection System (IDS) logs, firewall logs, paper
2640 reports, forms, clipboard checklists, digital records). These audit mechanisms should also be
2641 configured to work within reasonable time-frame boundaries, as defined by organizational
2642 policy. Organizations may encourage their system suppliers, developers, system integrators,
2643 external system service providers, and other ICT/OT-related service providers to do the same and
2644 may include in agreements requirements for such monitoring. However, organizations should not
2645 deploy audit mechanisms on systems outside of their organizational boundary, including those of
2646 suppliers, developers, system integrators, external system service providers, and other ICT/OT-
2647 related service providers.

2648 **AU-1    POLICY AND PROCEDURES**

2649     <u>Supplemental C-SCRM Guidance</u>: Organizations must designate a specific official to manage the
2650     development, documentation, and dissemination of the audit and accountability policy and procedures to
2651     include auditing of the supply chain information systems and network.  Audit mechanisms provide data for
2652     tracking activities in an organization's supply chain information systems and network. Audit and
2653     accountability policy and procedures should appropriately address such tracking and its availability for
2654     other various supply chain activities, such as configuration management. Suppliers, developers, system
2655     integrators, external system service providers, and other ICT/OT-related service providers activities should
2656     not be included in such policy, unless those are performed within the acquirer's supply chain information
2657     systems and network. Audit and accountability policy procedures should appropriately address supplier
2658     audits as a way to examine the quality of a particular supplier and the risk it presents to the organization
2659     and the organization's supply chain.

2660     <u>Level(s)</u>: 1, 2, 3

2661 **AU-2    EVENT LOGGING**

2662     <u>Supplemental C-SCRM Guidance</u>: An observable occurrence within the information system or supply
2663     chain network should be identified as a supply chain auditable event, based on the organization's SDLC
2664     context and requirements. Auditable events may include software/hardware changes, failed attempts to
2665     access supply chain information systems, or movement of source code. Information on such events should
2666     be captured by appropriate audit mechanisms and should be traceable and verifiable. Information captured
2667     may include type of event, date/time, length, and frequency of occurrence. Among other things, auditing
2668     may help detect misuse of the supply chain information systems or network caused by insider threat.  Logs
2669     are a key resource when identifying operational trends and long-term problems, and as such organizations
2670     should incorporate reviewing logs at contract renewal point for vendors to determine whether there is
2671     systemic problem.

2672    Level(s): 1, 2, 3
2673

2674    **AU-3    CONTENT OF AUDIT RECORDS**

2675    Supplemental C-SCRM Guidance: Audit records of a supply chain event should be handled and maintained
2676    in a manner that conforms to record retention requirements, preserves the integrity of the findings, and as
2677    appropriate, the confidentiality of the record information and its source(s).  In certain instances, such
2678    records may be used in administrative or legal proceedings.

2679    Level(s): 1, 2, 3

2680    **AU-6    AUDIT REVIEW, ANALYSIS, AND REPORTING**

2681    Supplemental C-SCRM Guidance: The organization should ensure that both supply chain and information
2682    security auditable events are appropriately filtered and correlated for analysis and reporting. For example, if
2683    new maintenance or a patch upgrade is recognized to have an invalid digital signature, the identification of
2684    the patch arrival qualifies as a supply chain auditable event, while invalid signature is an information
2685    security auditable event. The combination of these two events may provide information valuable to C-
2686    SCRM. The organization should adjust the level of audit record review based on risk changes (e.g., active
2687    threat intel, risk profile) on a specific vendor. Contracts should explicitly address how audit findings will be
2688    reported and adjudicated.
2689
2690    Level(s): 2, 3
2691
2692    Control Enhancement(s):

2693    **(9)**  *AUDIT REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM*
2694    *NONTECHNICAL SOURCES*

2695    Supplemental C-SCRM Guidance: In a C-SCRM context, nontechnical sources include changes to
2696    organizational security or operational policy, changes to procurement or contracting processes, and
2697    notifications from suppliers, developers, system integrators, external system service providers, and
2698    other ICT/OT-related service providers regarding plans to update, enhance, patch, or retire/dispose of a
2699    system/component.

2700    Level(s): 3

2701    **AU-10    NON-REPUDIATION**

2702    Supplemental C-SCRM Guidance: Organizations should implement non-repudiation techniques to protect
2703    both information systems and supply chain network. Examples of what may require non-repudiation
2704    include supply chain metadata describing the components, supply chain communication, delivery
2705    acceptance information, etc. For information systems, it can be patch or maintenance upgrades for software
2706    as well as component replacement in a large hardware system. Verifying that such components originate
2707    from the OEM is part of non-repudiation.

2708    Level(s): 3

2709    Control Enhancement(s):

2710    **(1)**  *NON-REPUDIATION | ASSOCIATION OF IDENTITIES*

2711    Supplemental C-SCRM Guidance: This enhancement helps traceability in cyber supply chain. It also
2712    facilitates the accuracy of provenance.

2713   Level(s): 2
2714

2715   **(2)** *NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY*

2716   Supplemental C-SCRM Guidance: This enhancement validates the relationship of provenance and a
2717   component within the supply chain. Therefore, it ensures integrity of provenance.

2718   Level(s): 2, 3

2719   **(3)** *NON-REPUDIATION | CHAIN OF CUSTODY*

2720   Supplemental C-SCRM Guidance: Chain of custody is fundamental to provenance and traceability in
2721   the cyber supply chain. It also helps verification of system and component integrity.

2722   Level(s): 2, 3

2723   **AU-12   AUDIT RECORD GENERATION**

2724   Supplemental C-SCRM Guidance: Organizations should ensure that audit record generation mechanisms
2725   are in place to capture all relevant supply chain auditable events. Examples of such events include:
2726   component version updates, component approvals from acceptance testing results, logistics data-capturing
2727   inventory, or transportation information.

2728   Level(s): 2, 3

2729   **AU-13   MONITORING FOR INFORMATION DISCLOSURE**

2730   Supplemental C-SCRM Guidance: Within the C-SCRM context, information disclosure may occur via
2731   multiple avenues including open source information. For example, supplier-provided errata may reveal
2732   information about an organization's system that may provide insight into the system that increases the risk
2733   to the system. Organizations should ensure monitoring is in place for contractor systems to detect
2734   unauthorized disclosure of any data and ensure contract language includes a requirement that the vendor
2735   will notify the organization, in accordance with organizationally-defined timeframes and as soon as
2736   possible in the event of any potential or actual unauthorized disclosure.

2737   Level(s): 2, 3

2738   **AU-14   SESSION AUDIT**

2739   Supplemental C-SCRM Guidance: Organizations should include non-federal contract employees in session
2740   audits to identify security risks in the supply chain.

2741   Level(s): 2, 3

2742   **AU-16   CROSS-ORGANIZATIONAL AUDIT LOGGING**

2743   Supplemental C-SCRM Guidance: In a C-SCRM context, this control includes the organization's use of
2744   system integrator or external service provider infrastructure. Organizations should add language to
2745   contracts on coordinating audit information requirements and information exchange agreements with
2746   vendors.

2747   Level(s): 2, 3

2748    <u>Control Enhancement(s):</u>

2749    **(2)**  *CROSS-ORGANIZATIONAL AUDIT LOGGING | SHARING OF AUDIT INFORMATION*
2750
2751    <u>Supplemental C-SCRM Guidance</u>: Whether managing a distributed audit environment or an audit data-
2752    sharing environment between organizations and its system integrators or external services providers,
2753    organizations should establish a set of requirements for the process of sharing audit information. In the
2754    case of the system integrator and external service provider and the organization, a service-level
2755    agreement of the type of audit data required vs. what can be provided must be agreed to in advance to
2756    ensure that the organization obtains the relevant audit information needed for ensuring that appropriate
2757    protections are in place to meet its mission operation protection needs. Ensure that coverage of both
2758    information systems and supply chain network are addressed for the collection and sharing of audit
2759    information.  Organizations should require its prime contractors to implement this control and flow
2760    down this requirement to relevant sub-level contractors.
2761
2762    <u>Level(s):</u> 2, 3
2763

**FAMILY: ASSESSMENT, AUTHORIZATION, AND MONITORING**

FIPS 200 specifies the Certification, Accreditation, and Security Assessments minimum security requirement as follows:

> *Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.*

Organizations should integrate C-SCRM, including the supply chain risk management process and the use of relevant controls defined in this publication, into ongoing security assessment and authorization activities. This includes activities to assess and authorize an organization's information systems, as well as external assessments of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, where appropriate. Cyber supply chain aspects include documentation and tracking of chain of custody and system interconnections within and between organizations, verification cyber supply chain security training, verification of suppliers claims of conformance to security, product/component integrity, and validation tools and techniques for noninvasive approaches to detecting counterfeits or malware (e.g., Trojans) using inspection for genuine components including manual inspection techniques.

**CA-1 POLICY AND PROCEDURES**

Supplemental C- SCRM Guidance: Integrate the development and implementation of assessment and authorization policies and procedures for cyber supply chain security into the control assessment and authorization policy, and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cyber supply chain risks, organizations should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the organization for conducting control assessment and authorization, any dependencies among those roles, and the interaction among the roles. Organization-wide security and privacy risk should be assessed on an ongoing basis and include supply chain risk assessment results.

Level(s): 1, 2, 3

**CA-2 CONTROL ASSESSMENTS**

Supplemental C-SCRM Guidance: Ensure that the control assessment plan incorporates relevant C-SCRM controls and control enhancements. The control assessment should cover the assessment of both information systems and the supply chain and ensure that an organization-relevant baseline set of controls and control enhancements are identified and used for the assessment. Control assessments can include information from supplier audits, reviews, and supply chain-related information. Organizations should develop a strategy for collecting information, including a strategy for engaging with providers on supply chain risk assessments. Such collaboration helps organizations leverage information from providers, reduce

2808    redundancy, identify potential courses of action for risk responses, and reduce the burden on providers. C-
2809    SCRM personnel should review the control assessment.

2810    Level(s): 2, 3

2811    Control Enhancement(s):

2812    **(2)**  *CONTROL ASSESSMENTS | SPECIALIZED ASSESSMENTS*

2813    Supplemental C-SCRM Guidance: Organizations should use a variety of assessment techniques and
2814    methodologies such as continuous monitoring, insider threat assessment, and malicious user's
2815    assessment. These assessment mechanisms are context-specific and require the organization to
2816    understand its supply chain and to define the required set of measures for assessing and verifying that
2817    appropriate protections have been implemented.
2818
2819    Level(s): 3

2820    **(3)**  *CONTROL ASSESSMENTS | LEVERAGING RESULTS FROM EXTERNAL ORGANIZATIONS*

2821    Supplemental C-SCRM Guidance: For C-SCRM, organizations should use external security
2822    assessments for suppliers, developers, system integrators, external system service providers, and other
2823    ICT/OT-related service providers. External assessments include certifications, third-party assessments,
2824    and, in the federal context, prior assessments performed by other departments and agencies.
2825    Organizations such as the International Organization for Standardization (ISO), the National
2826    Information Assurance Partnership (Common Criteria), and the Open Group Trusted Technology
2827    Forum (OTTF) certifications may also be used by non-federal and federal organizations alike, if such
2828    certifications meet agency needs.

2829    Level(s): 3

2830    **CA-3**    **INFORMATION EXCHANGE**

2831    Supplemental C-SCRM Guidance: Exchange of information or data between the system and other systems
2832    require scrutiny from a supply chain perspective. This includes understanding the interface characteristics
2833    and connections of those components/systems that are directly interconnected to or the data that is shared
2834    through those components/systems with developers, system integrators, external system service providers,
2835    other ICT/OT-related service providers and, in some cases, suppliers. Ensure that proper service-level
2836    agreements are in place to ensure compliance to system information exchange requirements defined by the
2837    organization, as the transfer of information between systems in different security or privacy domains with
2838    different security or privacy policies introduces risk that such transfers violate one or more domain security
2839    or privacy policies. Examples of such interconnections can include:
2840
2841        a.  A shared development and operational environment between the organization and system
2842            integrator;
2843        b.  Product update/patch management connection to an off-the-shelf supplier; and
2844        c.  Data request and retrieval transactions in a processing system residing on an external service
2845            provider shared environment.
2846
2847    Organizations should require its prime contractors to implement this control and flow down this
2848    requirement to relevant sub-tier contractors.

2849    Level(s): 3

2850    **CA-5**    **PLAN OF ACTION AND MILESTONES**

Supplemental C-SCRM Guidance: For system-level plan of actions and milestones (POA&Ms), organizations need to ensure that a separate POA&M exists for C-SCRM include both information systems and the supply chain. The C-SCRM POA&M should include tasks to be accomplished with a recommendation for completion before or after system authorization; resources required to accomplish the tasks; milestones established to meet the tasks; and the scheduled completion dates for the milestones and tasks. The organization should include in its C-SCRM POA&M relevant weaknesses, impact of weaknesses on information systems or the supply chain, any remediation to address weaknesses, and any continuous monitoring activities. The C-SCRM POA&M should be included as part of the authorization package.

Level(s): 2, 3

## CA-6     AUTHORIZATION

Supplemental C-SCRM Guidance: Authorizing officials should include C-SCRM in authorization decisions. To accomplish this, supply chain risks and compensating controls documented in C-SCRM Plans or system security plans, and C-SCRM plan of action and milestones should be included in the authorization package as part of the decision-making process. Risks should be determined and associated compensating controls selected based on output from criticality, threat, and vulnerability analyses. Authorizing officials may use guidance in Section 2 of this document as well as NISTIR 8179 to guide the assessment process.

Level(s): 1, 2, 3

## CA-7     CONTINUOUS MONITORING

Supplemental C-SCRM Guidance: For C-SCRM-specific guidance on this control, see Section 2 of this publication.

Level(s): 1, 2, 3

Control Enhancement(s):

**(3)** *CONTINUOUS MONITORING | TREND ANALYSES*

Supplemental C-SCRM Guidance: Information gathered during continuous monitoring/trend analysis serves as input into C-SCRM decisions including criticality analysis, vulnerability and threat analysis, and risk assessment. It also provides information that can be used in incident response and potentially can identify a cyber supply chain compromise, including insider threat.

Level(s): 3

2881    **FAMILY: CONFIGURATION MANAGEMENT**
2882
2883    FIPS 200 specifies the Configuration Management minimum security requirement as follows:
2884
2885        *Organizations must: (i) establish and maintain baseline configurations and inventories*
2886        *of organizational information systems (including hardware, software, firmware, and*
2887        *documentation) throughout the respective system development life cycles; and (ii)*
2888        *establish and enforce security configuration settings for information technology*
2889        *products employed in organizational information systems.*
2890
2891    Configuration Management helps track systems, components, and documentation within the
2892    information systems, networks, and throughout the SDLC. This is important for knowing what
2893    changes were made to those systems, components, and documentation, who made the changes,
2894    and who authorized the changes. Fundamentally, configuration management provides tools to
2895    establish the chain of custody for systems, components, and documentation. Configuration
2896    management also provides evidence for investigations of cyber supply chain compromise when
2897    determining which changes were authorized and which were not, and therefore provides useful
2898    information. Organizations should apply configuration management controls to their own
2899    systems and encourage use of configuration management controls by their suppliers, developers,
2900    system integrators, external system service providers, and other ICT/OT-related service
2901    providers. See NISTIR 7622 for more information on Configuration Management.
2902

2903    **CM-1    POLICY AND PROCEDURES**

2904        <u>Supplemental C-SCRM Guidance</u>: Configuration management impacts nearly every aspect of the cyber
2905        supply chain. Configuration Management is critical for organization's ability to establish provenance of
2906        components to include tracking and tracing them through the SDLC and through the supply chain. Properly
2907        defined and implemented configuration management capability provides greater assurance throughout the
2908        SDLC and the supply chain that components are authentic and have not been inappropriately modified.
2909        When defining configuration management policy and procedures, organizations should address the full
2910        SDLC. This should include procedures for introducing and removing components to and from the
2911        organization's information system boundary. Configuration Management policy should incorporate
2912        configuration items, data retention for configuration items and corresponding metadata, and tracking of the
2913        configuration item and its metadata. The organization should coordinate with suppliers, developers, system
2914        integrators, external system service providers, and other ICT/OT-related service providers regarding the
2915        configuration management policy.

2916        <u>Level(s):</u> 1, 2, 3

2917    **CM-2    BASELINE CONFIGURATION**

2918        <u>Supplemental C-SCRM Guidance</u>: Organizations should establish a baseline configuration of both the
2919        information system and the development environment including documenting, formally reviewing, and
2920        securing the agreement of stakeholders. The purpose of the baseline is to provide a starting point for
2921        tracking the changes to components, code, and/or settings throughout the SDLC.  Regular reviews and
2922        updates of baseline configurations (i.e., re-baselining) are critical for traceability and provenance.  The
2923        baseline configuration must take into consideration the organization's operational environment and any
2924        relevant suppliers', developers', system integrators', external system service providers', and other ICT/OT-
2925        related service providers' involvement within the organization's information systems and networks. If the

system integrator, for example, uses the existing organization's infrastructure, appropriate measures should be taken to establish a baseline that reflects an appropriate set of agreed-upon criteria for access and operation.

Level(s): 2, 3

Control Enhancement(s):

**(6)** *BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS*

Supplemental C-SCRM Guidance: The organization should maintain or require the maintenance of a baseline configuration of applicable suppliers', developers', system integrators', external system service providers', and other ICT/OT-related service providers' development, test (and if applicable, staging) environments as well as any configuration of interfaces.

Level(s): 2, 3

## CM-3   CONFIGURATION CHANGE CONTROL

Supplemental C-SCRM Guidance: Organizations should determine, implement, monitor, and audit configuration settings and change controls within the information systems and networks and throughout the SDLC. This control supports traceability for C-SCRM. The below NIST SP 800-53 Rev. 5 control enhancements CM-3 (1), (2), (4), and (8) are mechanisms that can be used for C-SCRM to collect and manage change control data.

Level(s): 2, 3

**(1)** *CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES*

Supplemental C-SCRM Guidance: Organizations should define a set of system changes that are critical to the protection of the information system and the underlying or interoperating systems and networks. These changes may be defined based on a criticality analysis (including components, processes, and functions) and where vulnerabilities exist that are not yet remediated (e.g., due to resource constraints). The change control process should also monitor for changes that may affect an existing security control to ensure that this control continues to function as required.

Level(s): 2, 3

**(2)** *CONFIGURATION CHANGE CONTROL | TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES*

Supplemental C-SCRM Guidance: Test, validate, and document changes to the system before finalizing the implementation of the changes.

Level(s): 2, 3

**(4)** *CONFIGURATION CHANGE CONTROL | SECURITY AND PRIVACY REPRESENTATIVES*

Supplemental C-SCRM Guidance: Require organization security and privacy representatives] to be members of the configuration change control function.

Level(s): 2, 3

**(8)** *CONFIGURATION CHANGE CONTROL | PREVENT OR RESTRICT CONFIGURATION CHANGES*

2967          Supplemental C-SCRM Guidance: Prevent or restrict changes to the configuration of the system under
2968          organization-defined circumstances.
2969
2970          Level(s): 2, 3

2971    **CM-4**    **IMPACT ANALYSIS**

2972          Supplemental C-SCRM Guidance: Organizations should take under consideration changes to the
2973          information system and underlying or interoperable systems and networks to determine whether the impact
2974          of these changes affects existing security control(s) and warrants additional or different protection to
2975          maintain an acceptable level of cyber supply chain risk. Ensure that stakeholders, such as system engineers
2976          and system security engineers are included in the impact analysis activities to provide their perspectives for
2977          C-SCRM. NIST SP 800-53 Rev. 5 control enhancement CM-4 (1) is a mechanism that can be used to
2978          protect the information system and from vulnerabilities that may be introduced through the test
2979          environment.
2980
2981          Level(s): 3

2982          **(1)** *IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS*

2983          Analyze changes to the system in a separate test environment before implementation in an operational
2984          environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or
2985          intentional malice
2986
2987          Level(s): 3
2988
2989          Related Control(s): SA-11, SC-7
2990

2991    **CM-5**    **ACCESS RESTRICTIONS FOR CHANGE**

2992          Supplemental C-SCRM Guidance: Organizations should ensure that requirements regarding physical and
2993          logical access restrictions for changes to the information systems and networks are defined and included in
2994          the organization's implementation of access restrictions. Examples include access restriction for changes to
2995          centrally managed processes for software component updates and the deployment of updates or patches.
2996
2997          Level(s): 2, 3
2998
2999          Control Enhancements:

3000          **(1)** *ACCESS RESTRICTIONS FOR CHANGE | AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS*

3001          Supplemental C-SCRM Guidance: Organizations should implement mechanisms to ensure automated
3002          access enforcement and auditing of the information system and the underlying systems and networks.
3003
3004          Level(s): 3

3005          **(6)** *ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES*

3006          Supplemental C-SCRM Guidance: Organizations should note that software libraries may be considered
3007          configuration items, access to which should be managed and controlled.
3008
3009          Level(s): 3

3010    **CM-6**    **CONFIGURATION SETTINGS**

Supplemental C-SCRM Guidance: Organizations should oversee the function of modifying configuration settings for their information systems and networks and throughout the SDLC. Methods of oversight include periodic verification, reporting, and review. Resulting information may be shared with various parties that have access to, are connected to, or engage in creation of the organization's information systems and networks on a need-to-know basis. Changes should be tested and approved before they are implemented. Configuration settings should be monitored and audited to alert designated organizational personnel when a change has occurred.

Level(s): 2, 3

Control Enhancement(s):

**(1)** *CONFIGURATION SETTINGS | AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION*

Supplemental C-SCRM Guidance: The organization should, when feasible, employ automated mechanisms to manage, apply, and verify configuration settings.

Level(s): 3

**(2)** *CONFIGURATION SETTINGS | RESPOND TO UNAUTHORIZED CHANGES*

Supplemental C-SCRM Guidance: The organization should ensure that designated security or IT personnel are alerted regarding unauthorized changes to configuration settings. When suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers are responsible for such unauthorized changes, this qualifies as a C-SCRM incident that should be recorded and tracked to monitor trends. For a more comprehensive view, a specific, predefined set of C-SCRM stakeholders should assess the cyber supply chain risk impact of unauthorized changes in the supply chain. When impact is assessed, relevant stakeholders should help define and implement appropriate mitigation strategies to ensure a comprehensive resolution.

Level(s): 3

## CM-7   LEAST FUNCTIONALITY

Supplemental C-SCRM Guidance: Least functionality reduces the attack surface of cyber supply chain risks. Organizations should select components that allow the flexibility and option for specifying and implementing least functionality. Organizations should ensure least functionality in their information systems and networks and throughout SDLC. NIST SP 800-53 Rev. 5 control enhancement CM-7 (9) mechanism can be used to protect information systems and networks from vulnerabilities that may be introduced by the use of unauthorized hardware being connected to organizational systems.

Level(s): 3

Control Enhancement(s):

**(1)** *LEAST FUNCTIONALITY | PERIODIC REVIEW*

Supplemental C-SCRM Guidance: Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

**(4)** *LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE*

Supplemental C-SCRM Guidance: Organizations should define requirements and deploy appropriate processes to specify and detect software that is not allowed. This can be aided by defining a

3057  requirement to, at a minimum, not use disreputable or unauthorized software. Organizations should
3058  require its prime contractors to implement this control and flow down this requirement to relevant sub-
3059  tier contractors.
3060
3061  Level(s): 2, 3

3062  **(5)** *LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE*

3063  Supplemental C-SCRM Guidance: Organizations should define requirements and deploy appropriate
3064  processes to specify allowable software. This can be aided by defining a requirement to use only
3065  reputable software. This can include requirements for alerts when new software and updates to
3066  software are introduced into the organization's environment. An example of such requirements is to
3067  allow open source software only if the code is available for an organization's evaluation and
3068  determined to be acceptable for use.
3069
3070  Level(s): 3

3071  **(6)** *LEAST FUNCTIONALITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES*

3072  Supplemental C-SCRM Guidance: The organization should ensure that code authentication
3073  mechanisms such as digital signatures are implemented when executing code to assure the integrity of
3074  software, firmware, and information of the information systems and networks.
3075
3076  Level(s): 2, 3

3077  **(7)** *LEAST FUNCTIONALITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS*

3078  Supplemental C-SCRM Guidance: The organization should obtain binary or machine-executable code
3079  directly from the OEM/developer or other acceptable, verified source.
3080
3081  Level(s): 3
3082

3083  **(8)** *LEAST FUNCTIONALITY | BINARY OR MACHINE EXECUTABLE CODE*

3084  Supplemental C-SCRM Guidance: When exceptions are made to use software products without
3085  accompanying source code or from sources with limited or no warranty because of compelling mission
3086  or operational requirements, approval by the authorizing official should be contingent upon the
3087  organization explicitly incorporating cyber supply chain risks in the assessment of such software
3088  products and the implementation of compensating controls to address any identified and assessed risks.
3089
3090  Level(s): 2, 3
3091

3092  **(9)** *LEAST FUNCTIONALITY | PROHIBITING THE USE OF UNAUTHORIZED HARDWARE*

3093  Organizations should define requirements and deploy appropriate processes to specify and detect
3094  hardware that is not allowed. This can be aided by defining a requirement to, at a minimum, not use
3095  disreputable or unauthorized hardware. Organizations should require its prime contractors to
3096  implement this control and flow down this requirement to relevant sub-tier contractors
3097
3098  Level(s): 2, 3
3099

3100  **CM-8   SYSTEM COMPONENT INVENTORY**

3101  Supplemental C-SCRM Guidance: Organizations should ensure that critical component assets within the
3102  information systems and networks are included in the asset inventory. The inventory must include
3103  information for critical component accountability.  Inventory information includes, for example, hardware
3104  inventory specifications, software license information, software version numbers, component owners, and
3105  for networked components or devices, machine names and network addresses. Inventory specifications
3106  include, for example, manufacturer, device type, model, serial number, and physical location.
3107
3108  Level(s): 2, 3
3109
3110  Control Enhancement(s):

3111  **(1)**  *SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATION AND REMOVAL*

3112      Supplemental C-SCRM Guidance: When installing, updating, or removing an information system,
3113      information system component, or network component, the organization needs to update the inventory
3114      to ensure traceability for tracking critical components. In addition, the information system's
3115      configuration needs to be updated to ensure an accurate inventory of supply chain protections, and re-
3116      baselined accordingly.
3117
3118      Level(s): 3

3119  **(2)**  *SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE*

3120      Supplemental C-SCRM Guidance: The organization should implement automated maintenance
3121      mechanisms to ensure that changes to component inventory for the information systems and networks
3122      are monitored for installation, update, and removal. When automated maintenance is performed with a
3123      predefined frequency and with the automated collation of relevant inventory information about each
3124      defined component, the organization should ensure that updates are available to relevant stakeholders
3125      for evaluation. Predefined frequencies for data collection should be less predictable in order to reduce
3126      the risk of an insider threat bypassing security mechanisms.
3127
3128      Level(s): 3

3129  **(4)**  *SYSTEM COMPONENT INVENTORY | ACCOUNTABILITY INFORMATION*

3130      Supplemental C-SCRM Guidance: The organization should ensure that accountability information is
3131      collected for information system and network components. The system/component inventory
3132      information should identify those individuals who originate an acquisition as well as intended end
3133      users, including any associated personnel who may administer or use the system/components.
3134
3135      Level(s): 3

3136  **(6)**  *SYSTEM COMPONENT INVENTORY | ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS*

3137      Supplemental C-SCRM Guidance: Assessed configurations and approved deviations must be
3138      documented and tracked. Any changes to the baseline configurations of information systems and
3139      networks require a review by relevant stakeholders to ensure that the changes do not result in increased
3140      cyber supply chain risk.
3141
3142      Level(s): 3

3143  **(7)**  *SYSTEM COMPONENT INVENTORY | CENTRALIZED REPOSITORY*

3144      Supplemental C-SCRM Guidance: Organizations may choose to implement centralized inventories that
3145      include components from all organizational information systems, networks, and their components.
3146      Centralized repositories of inventories provide opportunities for efficiencies in accounting for
3147      information systems, networks, and their components. Such repositories may also help organizations to
3148      rapidly identify the location and responsible individuals of components that have been compromised,

3149   breached, or are otherwise in need of mitigation actions. The organization should ensure that
3150   centralized inventories include supply chain-specific information required for proper component
3151   accountability (e.g., supply chain relevance and information system, network, or component owner).
3152
3153   Level(s): 3

3154   **(8)**  *SYSTEM COMPONENT INVENTORY | AUTOMATED LOCATION TRACKING*

3155   Supplemental C-SCRM Guidance: When employing automated mechanisms for tracking of
3156   information system components by physical location, the organization should incorporate information
3157   system, network, and component tracking needs to ensure accurate inventory.
3158
3159   Level(s): 2, 3

3160   **(9)**  *SYSTEM COMPONENT INVENTORY | ASSIGNMENT OF COMPONENTS TO SYSTEMS*

3161   Supplemental C-SCRM Guidance: When assigning components to systems, the organization should
3162   ensure that the information systems and networks with all relevant components are inventoried,
3163   marked, and properly assigned. This facilitates quick inventory of all components relevant to
3164   information systems and networks and enables tracking of components that are considered critical and
3165   require differentiating treatment as part of the information system and network protection activities.
3166
3167   Level(s): 3

3168   **CM-9   CONFIGURATION MANAGEMENT PLAN**

3169   Supplemental C-SCRM Guidance: Organizations should ensure that C-SCRM is incorporated into the
3170   configuration management planning activities.  Organizations should require its prime contractors to
3171   implement this control and flow down this requirement to relevant sub-tier contractors.
3172
3173   Level(s): 2, 3.
3174
3175   Control Enhancement(s):

3176   **(1)**  *CONFIGURATION MANAGEMENT PLAN | ASSIGNMENT OF RESPONSIBILITY*

3177   Supplemental C-SCRM Guidance: Organizations should ensure that all relevant roles are defined to
3178   address configuration management activities for information systems and networks. Organizations
3179   should ensure requirements and capabilities for configuration management are appropriately addressed
3180   or included in the following cyber supply chain activities: requirements definition, development,
3181   testing, market research and analysis, procurement solicitations and contracts, component installation
3182   or removal, system integration, operations, and maintenance.
3183
3184   Level(s): 2, 3
3185

3186   **CM-10  SOFTWARE USAGE RESTRICTIONS**

3187   Supplemental C-SCRM Guidance: Organizations should ensure that licenses for software used within their
3188   information systems and networks are documented, tracked, and maintained.   Tracking mechanisms should
3189   provide for the ability to trace users and use of licenses to access control information and processes.  As an
3190   example, when an employee is terminated, a "named user" license, should be revoked and license
3191   documentation should be updated to reflect this change.
3192
3193   Level(s): 2, 3

3194          Control Enhancement(s):

3195     **(1)**  *SOFTWARE USAGE RESTRICTIONS | OPEN-SOURCE SOFTWARE*

3196          Supplemental C-SCRM Guidance: When considering software, organizations should review all options
3197          and corresponding risks including open source or commercially licensed components. When using
3198          open source software (OSS), the organization should understand and review the open source
3199          communities' typical procedures regarding provenance, configuration management, sources, binaries,
3200          reusable frameworks, reusable libraries' availability for testing and use, and any other information that
3201          may impact cyber supply chain risk. Numerous open source solutions are currently in use by
3202          organizations, including in integrated development environments (IDEs) and web servers. The
3203          organization should:

3204

3205          a.   Track the use of OSS and associated documentation;
3206          b.   Ensure that the use of OSS adheres to the licensing terms and that these terms are acceptable to the
3207               organization
3208          c.   Document and monitor the distribution of software as it relates to licensing agreement to control
3209               copying and distribution; and
3210          d.   Evaluate and periodically audit the OSS's cyber supply chain as provided by the open source
3211               developer (e.g., information regarding provenance, configuration management, use of reusable
3212               libraries, etc.). This evaluation can be done reasonably easily by the organization through
3213               obtaining existing and often public documents as well as using experience based on software
3214               update and download processes in which the organization may have participated.

3215

3216          Level(s): 2, 3

3217     **CM-11   USER-INSTALLED SOFTWARE**

3218          Supplemental C-SCRM Guidance: This control extends to organizational information system and network
3219          users who are not employed by the organization. These users may be suppliers, developers, system
3220          integrators, external system service providers, and other ICT/OT-related service providers.
3221
3222          Level(s): 2, 3

3223     **CM-12   INFORMATION LOCATION**

3224          Supplemental C-SCRM Guidance:  Information residing in different physical locations may be subject to
3225          different cyber supply chain risks, depending on the specific location of the information.  Components
3226          originating or operating from different physical locations may also be subject to different supply chain
3227          risks, depending on the specific location of origination or operations.  Organizations should manage these
3228          risks through limiting access control, specifying allowable or disallowable geographic locations for
3229          backup/recovery, patching/upgrades, and information transfer/sharing.  NIST SP 800-53 Rev. 5 control
3230          enhancement CM-12 (1) is a mechanism that can be used to enable automated location of components.
3231
3232          Level(s): 2, 3
3233
3234          Control Enhancement(s):

3235     **(1)**  *INFORMATION LOCATION | AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION*

3236          Use automated tools to identify organization-defined information on organization-defined system
3237          components to ensure controls are in place to protect organizational information and individual
3238          privacy.
3239
3240          Level(s): 2, 3

3241    **CM-13   DATA ACTION MAPPING**

3242        Supplemental C-SCRM Guidance: In addition to personally identifiable information, understanding and
3243        documenting a map of system data actions for sensitive or classified information is necessary. Data action
3244        mapping should also be conducted to map internet of things (IoT) devices, embedded or stand-alone IoT
3245        systems, or IoT System of System data actions. Understanding what classified or IoT information is being
3246        processed, its sensitivity and/or effect on a physical thing or physical environment, how the sensitive or IoT
3247        information is being processed (e.g., if the data action is visible to an individual or is processed in another
3248        part of the system), and by whom provides a number of contextual factors that are important to assessing
3249        the degree of risk.  Data maps can be illustrated in different ways, and the level of detail may vary based on
3250        the mission and business needs of the organization. The data map may be an overlay of any system design
3251        artifact that the organization is using. The development of this map may necessitate coordination between
3252        program and security personnel regarding the covered data actions and the components that are identified
3253        as part of the system.
3254
3255        Level(s): 2, 3
3256

3257    **CM-14   SIGNED COMPONENTS**
3258
3259        Supplemental C-SCRM Guidance: Organizations should verify that the acquired hardware and software
3260        components are genuine and valid by using digitally signed components.  Verifying components before
3261        allowing installation helps organizations reduce cyber supply chain risks.
3262
3263        Level(s): 3

3264 **FAMILY: CONTINGENCY PLANNING**
3265

3266 FIPS 200 specifies the Contingency Planning minimum security requirement as follows:
3267

3268 *Organizations must establish, maintain, and effectively implement plans for emergency*
3269 *response, backup operations, and post-disaster recovery for organizational information*
3270 *systems to ensure the availability of critical information resources and continuity of*
3271 *operations in emergency situations.*
3272

3273 Cyber supply chain contingency planning includes planning for alternative suppliers of system
3274 components, alternative suppliers of systems and services, denial of service attacks to the supply
3275 chain, and planning for alternate delivery routes for critical system components. Such
3276 contingency plans help ensure existing service providers have an effective continuity of
3277 operations pan, especially, when the provider is delivering services in support of a critical
3278 mission function. Additionally, many techniques used for contingency planning, such as
3279 alternative processing sites, have their own cyber supply chains with their own attendant cyber
3280 supply chain risks. Organizations should ensure they understand and manage cyber supply chain
3281 risks and dependencies related to the contingency planning activities as necessary.

3282 **CP-1    POLICY AND PROCEDURES**

3283 Supplemental C-SCRM Guidance: Organizations should integrate C-SCRM into the contingency planning
3284 policy and related SCRM Strategy/Implementation Plan, policies, and SCRM Plan. The policy cover
3285 information systems and the supply chain network and, at a minimum, address scenarios such as:
3286     a.  Unplanned component failure and subsequent replacement;
3287     b.  Planned replacement related to feature improvements, maintenance, upgrades, and modernization;
3288        and
3289     c.  Product and/or service disruption.
3290
3291 Level(s): 1, 2, 3

3292 **CP-2    CONTINGENCY PLAN**

3293 Supplemental C-SCRM Guidance: Organizations should define and implement a contingency plan for the
3294 supply chain information systems and network to ensure preparations are in place to mitigate against the
3295 loss or degradation of data or operations. Contingencies should be put in place for the supply chain,
3296 network and information systems (especially critical components), and processes to ensure protection
3297 against compromise, provide appropriate failover, and timely recovery to an acceptable state of operations.
3298
3299 Level(s): 2, 3

3300 Control Enhancement(s):

3301   **(1)**  *CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS*

3302     Supplemental C-SCRM Guidance: Coordinate contingency plan development for supply chain risks
3303     with organizational elements responsible for related plans.
3304
3305     Level(S): 2, 3

3306   **(2)**  *CONTINGENCY PLAN | CAPACITY PLANNING*

3307    Supplemental C-SCRM Guidance: This enhancement helps availability of the supply chain network or
3308    information system components.
3309
3310    Level(s): 2, 3

3311    **(7)** *CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS*

3312    Supplemental C-SCRM Guidance: Organizations should ensure that supply chain network, information
3313    systems and components provided by an external service provider have appropriate failover (to include
3314    personnel, equipment, and network resources) to reduce or prevent service interruption or ensure
3315    timely recovery. Organizations should ensure that contingency planning requirements are defined as
3316    part of the service-level agreement. The agreement may have specific terms addressing critical
3317    components and functionality support in case of denial of service to ensure continuity of operation.
3318    Organizations should coordinate with external service providers to identify service providers' existing
3319    contingency plan practices and build on them as required by the organization's mission and business
3320    needs. Such coordination will aid in cost reduction and efficient implementation. Organizations should
3321    require its prime contractors that provide a mission/business-critical or -enabling service or product to
3322    implement this control and flow down this requirement to relevant sub-tier contractors.
3323
3324    Level(s): 3

3325    **(8)** *CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS*

3326    Supplemental C-SCRM Guidance: Ensure that critical assets (including hardware, software, and
3327    personnel) are identified to ensure that appropriate contingency planning requirements are defined and
3328    applied to ensure continuity of operation. A key step in this process is to complete a criticality analysis
3329    on components, functions, and processes to identify all critical assets. See Section 2 and NISTIR 8179
3330    for additional guidance on criticality analyses.
3331
3332    Level(s): 3

3333    **CP-3**    **CONTINGENCY TRAINING**

3334    Supplemental C-SCRM Guidance: Organizations should ensure that critical suppliers are included in
3335    contingency training.
3336
3337    Level(s): 2, 3

3338    Control Enhancement(s):

3339    **(1)** *CONTINGENCY TRAINING | SIMULATED EVENTS*

3340    Supplemental C-SCRM Guidance: Organizations should ensure that suppliers, developers, system
3341    integrators, external system service providers, and other ICT/OT-related service providers who have
3342    roles and responsibilities in providing critical services are included in contingency training exercises.
3343
3344    Level(s): 3

3345    **CP-4**    **CONTINGENCY PLAN TESTING**

3346    Supplemental C-SCRM Guidance: Organizations should ensure that critical suppliers are included in
3347    contingency testing.  The organization, in coordination with the service provider(s) should test whether
3348    continuity/resiliency capabilities, such as failover from a primary production site to a back-up site. perform
3349    as required. This testing may occur separately from a training exercise or be performed during the exercise.
3350    Organizations should reference their C-SCRM threat assessment output to develop scenarios to test how
3351    well the organization is able to withstand and/or recover from a C-SCRM threat event.

3352
3353　　　　　Level(s): 2, 3

3354　**CP-6　ALTERNATE STORAGE SITE**

3355　　　　　Supplemental C-SCRM Guidance: When managed by suppliers, developers, system integrators, external
3356　　　　　system service providers, and other ICT/OT-related service providers, alternate storage sites are considered
3357　　　　　within an organization's cyber supply chain network. Organizations should apply appropriate cyber supply
3358　　　　　chain controls to those storage sites.
3359
3360　　　　　Level(s): 2, 3

3361　　　　　Control Enhancement(s):

3362　　　　　**(1)** *ALTERNATE STORAGE SITE | SEPARATION FROM PRIMARY SITE*

3363　　　　　　　Supplemental C-SCRM Guidance: This enhancement helps resiliency of supply chain network,
3364　　　　　　　information systems, and information system components.
3365
3366　　　　　　　Level(s): 2, 3

3367　**CP-7　ALTERNATE PROCESSING SITE**

3368　　　　　Supplemental C-SCRM Guidance: When managed by suppliers, developers, system integrators, external
3369　　　　　system service providers, and other ICT/OT-related service providers, alternate storage sites are considered
3370　　　　　within an organization's cyber supply chain. Organizations should apply appropriate cyber supply chain
3371　　　　　controls to those processing sites.
3372
3373　　　　　Level(s): 2, 3

3374　**CP-8　TELECOMMUNICATIONS SERVICES**

3375　　　　　Supplemental C-SCRM Guidance: Organizations should incorporate alternate telecommunication service
3376　　　　　providers for their cyber supply chain and to support critical information systems.
3377
3378　　　　　Level(s): 2, 3

3379　　　　　Control Enhancement(s):

3380　　　　　**(3)** *TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS*

3381　　　　　　　Supplemental C-SCRM Guidance: Separation of primary and alternate providers supports cyber supply
3382　　　　　　　chain resilience.
3383
3384　　　　　　　Level(s): 2, 3

3385　　　　　**(4)** *TELECOMMUNICATIONS SERVICES | PROVIDER CONTINGENCY PLAN*

3386　　　　　　　Supplemental C-SCRM Guidance: For C-SCRM, suppliers, developers, system integrators, external
3387　　　　　　　system service providers, and other ICT/OT-related service providers contingency plans should
3388　　　　　　　provide separation in infrastructure, service, process, and personnel, where appropriate.
3389
3390　　　　　　　Level(s): 2, 3

3391　**CP-11　ALTERNATE COMMUNICATIONS PROTOCOLS**

3392          <u>Supplemental C-SCRM Guidance:</u> Organizations should ensure critical suppliers are included in
3393          contingency plans, training, and testing as part of incorporating alternate communications protocol
3394          capability to establish supply chain resilience.
3395
3396          <u>Level(s):</u> 2, 3
3397

3398
3399 **FAMILY: IDENTIFICATION AND AUTHENTICATION**
3400
3401 FIPS 200 specifies the Identification and Authentication minimum security requirement as
3402 follows:
3403
3404 *Organizations must identify information system users, processes acting on behalf of*
3405 *users, or devices and authenticate (or verify) the identities of those users, processes, or*
3406 *devices, as a prerequisite to allowing access to organizational information systems.*
3407
3408 NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems*
3409 *and Organizations,* expands the FIPS 200 identification and authentication control family to
3410 include identification and authentication of components, in addition to individuals (users) and
3411 processes acting on behalf of individuals within the cyber supply chain network. Identification
3412 and authentication is critical to C-SCRM because it provides traceability of individuals,
3413 processes acting on behalf of individuals, and specific systems/components in an organization's
3414 cyber supply chain network. Identification and authentication is required to appropriately
3415 manage cyber supply chain risks to both reduce risks of cyber supply chain compromise and to
3416 generate evidence in case of cyber supply chain compromise.
3417

3418 **IA-1    POLICY AND PROCEDURES**

3419     Supplemental C-SCRM Guidance: The organization should, at organizationally-defined intervals, review,
3420     enhance, and update their identity and access management policies and procedures to ensure that critical
3421     roles and processes within the supply chain network are defined and that the organization's critical systems,
3422     components, and processes are identified for traceability. This should include the identity of critical
3423     components that may not have been considered under identification and authentication in the past. Note
3424     that providing identification for all items within the supply chain would be cost-prohibitive, and discretion
3425     should be used. The organization should update related C-SCRM Strategy/Implementation Plan(s),
3426     Policies, and C-SCRM Plans.
3427
3428     Level(s): 1, 2, 3

3429 **IA-2    IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**

3430     Supplemental C-SCRM Guidance: Organizations should ensure that identification and requirements are
3431     defined and applied for organizational users accessing an ICT/OTsystem or supply chain network. An
3432     organizational user may include employees as well as individuals deemed to have the equivalent status of
3433     employees (e.g., contractors, guest researchers, etc.) and may include system integrators fulfilling
3434     contractor roles. Criteria such as "duration in role" can aid in defining which identification and
3435     authentication mechanisms are used. The organization may choose to define a set of roles and associate a
3436     level of authorization to ensure proper implementation.
3437
3438     Level(s): 1, 2, 3

3439 **IA-3    DEVICE IDENTIFICATION AND AUTHENTICATION**

3440     Supplemental C-SCRM Guidance: Organizations should implement capabilities to distinctly and positively
3441     identify devices and software within their supply chain and, once identified, be able to verify that the
3442     identity is authentic. Devices that require unique device-to-device identification and authentication should

3443      be defined by type, by device, or by a combination of type and device. Software that requires authentication
3444      should be identified through a software identification tag (SWID) that enables verification of the software
3445      package and authentication of the organization releasing the software package.
3446
3447      Level(s): 1, 2, 3

3448      **IA-4**      **IDENTIFIER MANAGEMENT**

3449      Supplemental C-SCRM Guidance: Identifiers allow for greater discoverability and traceability. Within the
3450      organization's cyber supply chain, identifiers should be assigned to systems, individuals, documentation,
3451      devices, and components. In some cases, identifiers may be maintained throughout a system's life cycle,
3452      from concept to retirement, but at a minimum throughout the system's life within the organization.
3453
3454      For software development, identifiers should be assigned for those components that have achieved
3455      configuration item recognition. For devices and operational systems, identifiers should be assigned when
3456      the items enter the organization's supply chain, such as when they are transferred to the organization's
3457      ownership or control through shipping and receiving or via download.
3458
3459      Suppliers, developers, system integrators, external system service providers, and other ICT/OT-related
3460      service providers typically use their own identifiers for tracking purposes within their own supply chain.
3461      Organizations should correlate those identifiers with the organization-assigned identifiers for traceability
3462      and accountability.
3463
3464      Level(s): 2, 3
3465
3466      Related Controls: IA-3 (1), IA-3 (2), IA-3 (3), and IA-3 (4)

3467      Control Enhancement(s):

3468      **(6)**   *IDENTIFIER MANAGEMENT | CROSS-ORGANIZATION MANAGEMENT*

3469      Supplemental C-SCRM Guidance: This enhancement helps traceability and provenance of elements
3470      within the cyber supply chain, through the coordination of identifier management among the
3471      organization and its suppliers, developers, system integrators, external system service providers, and
3472      other ICT/OT-related service providers. This includes information systems and components as well as
3473      individuals engaged in supply chain activities.
3474
3475      Level(s): 1, 2, 3

3476      **IA-5**      **AUTHENTICATOR MANAGEMENT**

3477      Supplemental C-SCRM Guidance: This control facilitates traceability and non-repudiation throughout the
3478      cyber supply chain.
3479
3480      Level(s): 2, 3

3481      Control Enhancement(s):

3482      **(5)**   *AUTHENTICATOR MANAGEMENT | CHANGE AUTHENTICATORS PRIOR TO DELIVERY*

3483      Supplemental C-SCRM Guidance: This enhancement provides verification of chain of custody within
3484      the organization's cyber supply chain.
3485
3486      Level(s): 3

3487      **(9)**   *AUTHENTICATOR MANAGEMENT | FEDERATED CREDENTIAL MANAGEMENT*

3488        Supplemental C-SCRM Guidance: This enhancement facilitates provenance and chain of custody
3489        within the organization's cyber supply chain.
3490
3491        Level(s): 3

3492    **IA-8**    **IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)**

3493        Supplemental C-SCRM Guidance: Suppliers, developers, system integrators, external system service
3494        providers, and other ICT/OT-related service providers have the potential to engage the organization's
3495        supply chain for service delivery (development/integration services, product support, etc.). Organizations
3496        should manage the establishment, auditing, use, and revocation of identification credentials and
3497        authentication of non-organizational users within the \ supply chain. Organizations should ensure
3498        promptness in performing identification and authentication activities, especially in the case of revocation
3499        management, to help mitigate against cyber supply chain risks such as insider threat.
3500
3501        Level(s): 2, 3

3502    **IA-9**    **SERVICE IDENTIFICATION AND AUTHENTICATION**

3503        Supplemental C-SCRM Guidance: Organizations should ensure that identification and authentication is
3504        defined and managed for access to services (i.e., web applications using digital certificates or services or
3505        applications that query a database as opposed to labor-services) throughout the supply chain.  Organizations
3506        should ensure they know what services are being procured and from whom. Services procured should be
3507        listed on a validated list of services for the organization or have compensating controls in place.
3508
3509        Level(s): 2, 3

3510 **FAMILY: INCIDENT RESPONSE**
3511
3512 FIPS 200 specifies the Incident Response minimum security requirement as follows:
3513
3514     *Organizations must: (i) establish an operational incident handling capability for*
3515     *organizational information systems that includes adequate preparation, detection,*
3516     *analysis, containment, recovery, and user response activities; and (ii) track, document,*
3517     *and report incidents to appropriate organizational officials and/or authorities.*
3518
3519 Cyber supply chain compromises may span suppliers, developers, system integrators, external
3520 system service providers, and other ICT/OT-related service providers. Organizations should
3521 ensure their incident response controls address C-SCRM including what, when and how
3522 information about incidents will be reported or shared by, with, or between suppliers, developers,
3523 system integrators, external system service providers, other ICT/OT-related service providers,
3524 and any relevant interagency bodies. Incident response will help determine whether an incident is
3525 related to the cyber supply chain.
3526

3527 **IR-1    POLICY AND PROCEDURES**

3528     <u>Supplemental C-SCRM Guidance</u>: Organizations should integrate C-SCRM into incident response policy
3529     and procedures, and related C-SCRM Strategy/Implementation Plan(s), Policies, and C-SCRM Plan. Policy
3530     and procedures must provide direction about how to address supply chain related incidents and those
3531     cybersecurity incidents that may complicate or impact the cyber supply chain. Individuals working within
3532     specific mission and system environments need to recognize cyber supply chain-related incidents. Incident
3533     response policy should state when and how threats and incidents should be handled, reported, and
3534     managed.
3535
3536     Additionally, the policy should define when, how, and with whom to communicate to the FASC (Federal
3537     Acquisition Security Council), and other stakeholders or partners within the broader supply chain in the
3538     event of a cyber threat or incident. Departments and agencies must notify the FASC of supply chain risk
3539     information when 1) the FASC requests information relating to a particular source, covered article or
3540     procures; or 2) an executive agency has determined there is a reasonable basis to conclude a substantial
3541     supply chain risk associated with a source, covered procurement, or covered article exists. In such
3542     instances, the executive agency shall provide the FASC with relevant information concerning the source or
3543     covered article, including: (i) supply chain risk information identified through the course of the agency's
3544     activities in furtherance of mitigating, identifying or managing its supply chain risk; and (ii) supply chain
3545     risk information regarding covered procurement actions by the agency under the Federal Acquisition
3546     Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency
3547     under 41 U.S.C. § 4713.  Bidirectional communication with supply chain partners should be defined in
3548     agreements with suppliers, developers, system integrators, external system service providers, and other
3549     ICT/OT-related service providers to inform all involved parties of a cyber supply chain incident. Incident
3550     information may also be shared with organizations such as the Federal Bureau of Investigation (FBI), US
3551     CERT (United States Computer Emergency Readiness Team), and the NCCIC (National Cybersecurity and
3552     Communications Integration Center) as appropriate. Depending on the severity of the incident, the need for
3553     accelerated communications up and down the supply chain may be necessary. Appropriate agreements
3554     should be put in place with suppliers, developers, system integrators, external system service providers, and
3555     other ICT/OT-related service providers to ensure speed of communication, response, corrective actions, and
3556     other related activities.  Organizations should require its prime contractors to implement this control and
3557     flow down this requirement to relevant sub-tier contractors.
3558

In Levels 2 and 3, procedures and organization-specific incident response methods must be in place, training completed (consider including Operations Security (OPSEC) and any appropriate threat briefing in training), and coordinated communication established throughout the supply chain to ensure an efficient and coordinated incident response effort.

Level(s): 1, 2, 3

Control Enhancement(s):

**(1)**  *POLICY AND PROCEDURES | C-SCRM INCIDENT INFORMATION SHARING*

Organizations should ensure that their incident response policies and procedures provide guidance on effective information sharing of incidents and other key risk indicators in the cyber supply chain. Guidance should at a minimum cover the collection, synthesis, and distribution of incident information from a diverse set of data sources such as publicly data repositories, paid subscription services, and in-house threat intelligence teams.

Organizations operating in the public sector should include specific guidance on when and how to communicate with interagency partnerships such as the FASC (Federal Acquisition Security Council) and other stakeholders or partners within the broader supply chain in the event of a cyber threat or incident.

Departments and agencies must notify the FASC of supply chain risk information when
1) The FASC requests information relating to a particular source, covered article or procures; or
2) An executive agency has determined there is a reasonable basis to conclude a substantial supply chain risk associated with a source, covered procurement, or covered article exists.

In such instances, the executive agency shall provide the FASC with relevant information concerning the source or covered article, including:
i.       Supply chain risk information identified through the course of the agency's activities in furtherance of mitigating, identifying or managing its supply chain risk; and
ii.      Supply chain risk information regarding covered procurement actions by the agency under the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA) 41 U.S.C. § 4713; and any orders issued by the agency under 41 U.S.C. § 4713.

Level(s): 1, 2, 3

**IR-2     INCIDENT RESPONSE TRAINING**

Supplemental C-SCRM Guidance: Organizations should ensure that critical suppliers are included in incident response training.

Level(s): 2, 3

**IR-3     INCIDENT RESPONSE TESTING**

Supplemental C-SCRM Guidance: Organizations should ensure that critical suppliers are included in and/or provided incident response testing.

Level(s): 2, 3

**IR-4     INCIDENT HANDLING**

Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance provided in control enhancements.

3605
3606        Level(s): 1,2,3

3607        Control Enhancement(s):

3608        **(6)**  *INCIDENT HANDLING | INSIDER THREATS*

3609        Supplemental C-SCRM Guidance: This enhancement helps limit exposure of the C-SCRM information
3610        systems, networks, and processes to insider threats. Organizations should ensure that insider threat
3611        incident handling capabilities account for the potential of insider threats associated with suppliers,
3612        developers, system integrators, external system service providers, and other ICT/OT-related service
3613        providers' personnel with access to ICT/OT systems within the authorization boundary.

3614        Level(s): 1, 2, 3

3615        **(7)**  *INCIDENT HANDLING | INSIDER THREATS - INTRA-ORGANIZATION*

3616        Supplemental C-SCRM Guidance: This enhancement helps limit exposure of C-SCRM information
3617        systems, networks, and processes to insider threats.  Organizations should ensure that insider threat
3618        coordination includes suppliers, developers, system integrators, external system service providers, and
3619        other ICT/OT-related service providers.

3620        Level(s): 1, 2, 3

3621        **(10)** *INCIDENT HANDLING | SUPPLY CHAIN COORDINATION*

3622        Supplemental C-SCRM Guidance: A number of organizations may be involved in managing incidents
3623        and responses for supply chain security. After an initial processing of the incident is completed and a
3624        decision is made to take action (in some cases, the action may be "no action"), the organization may
3625        need to coordinate with their suppliers, developers, system integrators, external system service
3626        providers, other ICT/OT-related service providers, and any relevant interagency bodies to facilitate
3627        communications, incident response, root cause, and corrective actions activities. Organizations should
3628        securely share information through a coordinated set of personnel in key roles to allow for a more
3629        comprehensive incident handling approach. Selecting suppliers, developers, system integrators,
3630        external system service providers, and other ICT/OT-related service providers with mature capabilities
3631        for supporting cyber supply chain incident handling is important for reducing cyber supply chain risk.
3632        If transparency for incident handling is limited due to the nature of the relationship, define a set of
3633        acceptable criteria in the agreement (e.g., contract). A review (and potential revision) of the agreement
3634        is recommended, based on the lessons learned from previous incidents. Organizations should require
3635        its prime contractors to implement this control and flow down this requirement to relevant sub-tier
3636        contractors.
3637
3638        Level(s): 2

3639        **(11)** *INCIDENT HANDLING | INTEGRATED INCIDENT RESPONSE TEAM*

3640        Supplemental C-SCRM Guidance: An organization should include a forensics team and/or capability
3641        as part of an integrated incident response team for supply chain incidents. Where relevant and
3642        practical, integrated incident response teams should also include necessary geographical representation
3643        as well as suppliers, developers, system integrators, external system service providers, and other
3644        ICT/OT-related service providers.

3645        Level(s): 3

3646   **IR-5    INCIDENT MONITORING**

3647 Supplemental C-SCRM Guidance: Organizations should ensure agreements with suppliers include
3648 requirements to track and document incidents and response decisions and activities.
3649
3650 Level(s): 2, 3

3651 **IR-6    INCIDENT REPORTING**

3652 Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance provided in control
3653 enhancement IR-6 (3).
3654
3655 Level(s): 3
3656
3657 Control Enhancement(s):

3658 **(3)** *INCIDENT REPORTING | SUPPLY CHAIN COORDINATION*

3659 Supplemental C-SCRM Guidance: Communications of security incident information from the
3660 organization to suppliers, developers, system integrators, external system service providers, and other
3661 ICT/OT-related service providers or vice-verse requires protection. The organization should ensure
3662 that information is reviewed and approved for sending based on its agreements with the suppliers and
3663 any relevant interagency bodies. Any escalation of or exception from this reporting should be clearly
3664 defined in the agreement. The organization should ensure that incident reporting data is adequately
3665 protected for transmission and received by approved individuals only. Organizations should require its
3666 prime contractors to implement this control and flow down this requirement to relevant sub-tier
3667 contractors.
3668
3669 Level(s): 3

3670 **IR-7    INCIDENT RESPONSE ASSISTANCE**

3671 Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance provided in control
3672 enhancement IR-7 (2).
3673
3674 Level(s): 3
3675
3676 Control Enhancement(s):

3677 **(1)** *INCIDENT RESPONSE ASSISTANCE | COORDINATION WITH EXTERNAL PROVIDERS*

3678 Supplemental C-SCRM Guidance: Organization's agreements with prime contractors should specify
3679 the conditions under which a government-approved or -designated third party will be available or may
3680 be required to provide assistance with incident response, as well as describe the role and responsibility
3681 of that third party.
3682
3683 Level(s): 3

3684 **IR-8    INCIDENT RESPONSE PLAN**

3685 Supplemental C-SCRM Guidance: Organizations should coordinate, develop, and implement an incident
3686 response plan that includes information sharing responsibilities with critical suppliers and, in a federal
3687 context, interagency partners and the FASC. Organizations should require its prime contractors to
3688 implement this control and flow down this requirement to relevant sub-tier contractors.
3689
3690 Related Control(s): IR-10
3691
3692 Level(s): 2, 3

3693    **IR-9    INFORMATION SPILLAGE RESPONSE**

3694    <u>Supplemental C-SCRM Guidance</u>: The supply chain is vulnerable to information spillage. The organization
3695    should include supply chain-related information spills in its information spillage response plan. This may
3696    require coordination with suppliers, developers, system integrators, external system service providers, and
3697    other ICT/OT-related service providers. The details of how this coordination is to be conducted should be
3698    included in the agreement (e.g., contract). Organizations should require its prime contractors to implement
3699    this control and flow down this requirement to relevant sub-tier contractors.
3700
3701    <u>Level(s)</u>: 3
3702
3703    <u>Related Controls</u>: SA-4
3704

3705 **FAMILY: MAINTENANCE**
3706
3707 FIPS 200 specifies the Maintenance minimum security requirement as follows:
3708
3709 *Organizations must: (i) perform periodic and timely maintenance on organizational*
3710 *information systems; and (ii) provide effective controls on the tools, techniques,*
3711 *mechanisms, and personnel used to conduct information system maintenance.*
3712
3713 Maintenance is frequently performed by an entity that is separate from the organization. As
3714 such, maintenance becomes part of the supply chain. Maintenance includes performing updates
3715 and replacements. C-SCRM should be applied to maintenance situations including assessing
3716 the cyber supply chain risks, selecting C-SCRM controls, implementing these controls, and
3717 monitoring them for effectiveness.
3718

3719 **MA-1    POLICY AND PROCEDURES**

3720       Supplemental C-SCRM Guidance: Organizations should ensure that C-SCRM is included in maintenance
3721       policies and procedures, and related SCRM Strategy/Implementation Plan, SCRM Policies, and SCRM
3722       Plan(s) for all organizational information systems and networks. With many maintenance contracts,
3723       information on mission, organization, and system-specific objectives and requirements is shared between
3724       the organization and its suppliers, developers, system integrators, external system service providers, and
3725       other ICT/OT-related service providers, allowing for vulnerabilities and opportunities for attack. In many
3726       cases, the maintenance of systems is outsourced to a system integrator and as such, appropriate measures
3727       must be taken. Even when maintenance is not outsourced, the upgrades and patches, frequency of
3728       maintenance, replacement parts, and other aspects of system maintenance are affected by the supply chain.
3729
3730       Maintenance policies should be defined both for the system and the network. The maintenance policy
3731       should reflect controls based on a risk assessment (including criticality analysis), including controls such as
3732       remote access, roles and attributes of maintenance personnel that have access, the frequency of updates,
3733       duration of contract, logistical path and method used for updates or maintenance, and monitoring and audit
3734       mechanisms. The maintenance policy should state which tools are explicitly allowed or not allowed. For
3735       example, in the case of software maintenance, source code, test cases, and other item accessibility to
3736       maintain a system or components should be stated in the contract.
3737
3738       Maintenance policies should be refined and augmented at each level. At Level 1, the policy should
3739       explicitly assert that C-SCRM should be applied throughout the SDLC, including maintenance activities.
3740       At Level 2, the policy should reflect the mission operation's needs and critical functions. At Level 3 it
3741       should reflect the specific system needs. The requirements in Level 1, such as nonlocal maintenance,
3742       should flow to Levels 2 and 3; for example, when nonlocal maintenance is not allowed by Level 1, it
3743       should also not be allowed at Levels 2 and 3.
3744
3745       The organization should communicate applicable maintenance policy requirements to relevant prime
3746       contractors and require they implement this control and flow down this requirement to relevant sub-tier
3747       contractors.
3748
3749       Level(s): 1, 2, 3

3750 **MA-2    CONTROLLED MAINTENANCE**

3751       Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance is provided in control
3752       enhancement MA-2 (2).

3753
3754    Control Enhancement(s):

3755    **(2)** *CONTROLLED MAINTENANCE | AUTOMATED MAINTENANCE ACTIVITIES*

3756
3757    Supplemental C-SCRM Guidance: Organizations should ensure that all automated maintenance
3758    activities for supply chain systems and networks are controlled and managed according to the
3759    maintenance policy. Examples of automated maintenance activities can include COTS product patch
3760    updates, call home features with failure notification feedback, etc. Managing these activities may
3761    require establishing staging processes with appropriate supporting mechanisms to provide vetting or
3762    filtering as appropriate. Staging processes may be especially important for critical systems and
3763    components.
3764
3765    Level(s): 3

3766    **MA-3   MAINTENANCE TOOLS**

3767    Supplemental C-SCRM Guidance: Maintenance tools are considered part of the supply chain. They also
3768    have a supply chain of their own. C-SCRM should be integrated when the organization acquires or
3769    upgrades a maintenance tool (e.g., an update to development environment or testing tool), including during
3770    the selection, ordering, storage, and integration of the maintenance tool. The organization should perform
3771    continuous review and approval of maintenance tools, to include those maintenance tools in use by external
3772    service providers. The organization should also integrate C-SCRM when evaluating replacement parts for
3773    maintenance tools. This control may be performed at both Levels 2 and 3, depending on how an agency
3774    handles the acquisition, operations, and oversight of maintenance tools.
3775
3776    Level(s): 2, 3.
3777
3778    Control Enhancement(s):

3779    **(1)** *MAINTENANCE TOOLS | INSPECT TOOLS*

3780    Supplemental C-SCRM Guidance: The organization should deploy acceptance testing to verify that the
3781    maintenance tools of the ICT supply chain infrastructure are as expected. Maintenance tools should be
3782    authorized with appropriate paperwork, verified as claimed through initial verification, and tested for
3783    vulnerabilities, appropriate security configurations, and stated functionality.
3784
3785    Level(s): 3

3786    **(2)** *MAINTENANCE TOOLS | INSPECT MEDIA*

3787    Supplemental C-SCRM Guidance: The organization should verify that the media containing diagnostic
3788    and test programs that suppliers use on the organization's information systems operate as expected and
3789    provide only required functions. Use of media from maintenance tools should be consistent with
3790    organization's policies and procedures and pre-approved. Organizations should also ensure the
3791    functionality does not exceed that which was agreed upon.
3792
3793    Level(s): 3

3794    **(3)** *MAINTENANCE TOOLS | PREVENT UNAUTHORIZED REMOVAL*

3795    Supplemental C-SCRM Guidance: Unauthorized removal of systems and network maintenance tools
3796    from the cyber supply chain may introduce supply chain risk including, for example, unauthorized
3797    modification, replacement with counterfeit, or malware insertion while the tool is outside of the
3798    organization's control. Systems and network maintenance tools can include integrated development
3799    environment (IDE), testing, or vulnerability scanning. For C-SCRM, it is important that organizations

3800  should explicitly authorize, track, and audit any removal of maintenance tools. Once systems and
3801  network tools are allowed access to an organization/information system, they should remain the
3802  property/asset of the system owner and tracked if removed and used elsewhere in the organization. ICT
3803  maintenance tools either currently in use or in storage should not be allowed to leave the organization's
3804  premises until they are properly vetted for removal (i.e., maintenance tool removal should not exceed
3805  in scope what was authorized for removal, and should be completed in accordance with the
3806  organization's established policies and procedures).
3807
3808  Level(s): 3

3809  **MA-4  NONLOCAL MAINTENANCE**

3810  Supplemental C-SCRM Guidance: Nonlocal maintenance may be provided by contractor personnel.
3811  Appropriate protections should be in place to manage associated risks. Controls applied to internal
3812  maintenance personnel are applied to any suppliers, developers, system integrators, external system service
3813  providers, and other ICT/OT-related service providers performing a similar maintenance role and enforced
3814  through contractual agreements with their external service providers.
3815
3816  Level(s): 2, 3
3817
3818  Control Enhancement(s):

3819  **(3)** *NONLOCAL MAINTENANCE | COMPARABLE SECURITY AND SANITIZATION*

3820  Supplemental C-SCRM Guidance: Should any nonlocal maintenance or diagnostic services be
3821  performed to systems components or systems by suppliers, developers, system integrators, external
3822  system service providers, and other ICT/OT-related service providers, the organization should ensure
3823  that:
3824  • Appropriate measures are taken to verify that the nonlocal environment meets appropriate
3825  security levels for maintenance and diagnostics per agreements between the organization and
3826  vendor;
3827  • Appropriate levels of sanitizing are completed to remove any organization-specific data
3828  residing in components; and
3829  • Appropriate diagnostics are completed to ensure that components are sanitized, preventing
3830  malicious insertion prior to returning to the organizational system and or supply chain
3831  network.
3832
3833  The organization should require its prime contractors to implement this control and flow down this
3834  requirement to relevant sub-tier contractors.
3835
3836  Level(s): 2, 3

3837  **MA-5  MAINTENANCE PERSONNEL**

3838  Supplemental C-SCRM Guidance: Maintenance personnel may be employed by a supplier, developer,
3839  system integrators, external system service providers, or other ICT/OT-related service providers. As such,
3840  appropriate protections should be in place to manage associated risks.  The same controls applied to
3841  internal maintenance personnel should be applied to any contractor personnel performing a similar
3842  maintenance role and enforced through contractual agreements with their external service providers.
3843
3844  Level(s): 2, 3
3845
3846  Control Enhancement(s):

3847  **(4)** *MAINTENANCE PERSONNEL | FOREIGN NATIONALS*

Supplemental C-SCRM Guidance: Vetting of foreign nationals with access to critical non-national security systems/services must take C-SCRM into account and be extended to all relevant contractor personnel. Organizations should specify in agreements any restrictions or vetting requirements that pertain to foreign nationals and flow requirement down to relevant sub-contractors.

Level(s): 2, 3

**MA-6   TIMELY MAINTENANCE**

Supplemental C-SCRM Guidance: For spare parts, replacement parts, or alternate sources, the organization should purchase through original equipment manufacturers (OEMs), authorized distributors or authorized reseller and ensure appropriate lead times. If OEMs are not available, it is preferred to acquire from authorized distributors. If an OEM or an authorized distributor is not available, then it is preferred to acquire from an authorized reseller. Organizations should obtain verification on whether the distributor or reseller is authorized. Where possible, organizations should use an authorized distributor/dealer approved list. If the only alternative is to purchase from a non-authorized distributor or secondary market, a risk assessment should be performed, including a revisit of criticality and threat analysis to identify additional risk mitigations to be used. For example, the organization should check the source of supply for history of counterfeits, inappropriate practices, or a criminal record. See Section 2 for criticality and threat analysis details. The organization should maintain a bench stock of critical OEM parts, if feasible, when acquisition of such parts may not be able to be accomplished within needed timeframes.

Level(s): 3

**MA-7   FIELD MAINTENANCE**

Supplemental C-SCRM Guidance: Organizations should use trusted facilities when additional rigor and quality control checks are needed, if at all practical or possible. Trusted facilities should be on an approved list and have additional controls in place.

Related Control(s): MA-2, MA-4, MA-5.

Level(s): 3

**MA-8   MAINTENANCE MONITORING AND INFORMATION SHARING (NEW)**

Control: The organization monitors the status of systems and components, and communicates out-of-bounds and out-of-spec performance to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. The organization should also report this information to the Government-Industry Data Exchange Program (GIDEP).

Supplemental C-SCRM Guidance: Tracking failure rates of components provides useful information to the acquirer to help plan for contingencies, alternate sources of supply, and replacements. Failure rates are also useful for monitoring quality and reliability of systems and components. This information provides useful feedback to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers for corrective action and continuous improvement. In Level 2, agencies should track and communicate the failure rates to suppliers (OEM and/or an authorized distributor). The failure rates and the issues that can indicate failures including root causes should be identified by an organization's technical personnel (e.g., developers, administrators, or maintenance engineers) in Level 3 and communicated to Level 2. These individuals are able to verify the problem and identify technical alternatives.

Related Control(s): IR-4(10).

Level(s): 3

3897
3898 **FAMILY: MEDIA PROTECTION**
3899
3900 FIPS 200 specifies the Media Protection minimum security requirement as follows:
3901
3902 　　　*Organizations must: (i) protect information system media, both paper and digital; (ii)*
3903 　　　*limit access to information on information system media to authorized users; and (iii)*
3904 　　　*sanitize or destroy information system media before disposal or release for reuse.*
3905
3906 Media itself can be a component traversing the cyber supply chain or containing information
3907 about the organization's cyber supply chain. This includes both physical and logical media
3908 including, for example, system documentation on paper or in electronic files, shipping and
3909 delivery documentation with acquirer information, memory sticks with software code, or
3910 complete routers or servers that include permanent media. The information contained on the
3911 media may be sensitive or proprietary information. Additionally, the media is used throughout
3912 the SDLC, from concept to disposal. Organizations should ensure that Media Protection controls
3913 are applied to both an organization's media and the media received from suppliers, developers,
3914 system integrators, external system service providers, and other ICT/OT-related service
3915 providers throughout the SDLC.
3916

3917 **MP-1　POLICY AND PROCEDURES**

3918 　　　Supplemental C-SCRM Guidance: Various documents and information on a variety of physical and
3919 　　　electronic media are disseminated throughout the cyber supply chain. This information may contain a
3920 　　　variety of sensitive information and intellectual property from suppliers, developers, system integrators,
3921 　　　external system service providers, and other ICT/OT-related service providers and should be appropriately
3922 　　　protected. Media protection policies and procedures should address cyber supply chain concerns including
3923 　　　media in the organization's cyber supply chain, as well as media throughout the SDLC.
3924
3925 　　　Level(s): 1, 2

3926 **MP-4　MEDIA STORAGE**

3927 　　　Supplemental C-SCRM Guidance: Media storage controls should include C-SCRM activities.
3928 　　　Organizations should specify and include in agreements (e.g., contracting language) media storage policies
3929 　　　for their suppliers, developers, system integrators, external system service providers, and other ICT/OT-
3930 　　　related service providers. The organization should require its prime contractors to implement this control
3931 　　　and flow down this requirement to relevant sub-tier contractors.
3932
3933 　　　Level(s): 1, 2

3934 **MP-5　MEDIA TRANSPORT**

3935 　　　Supplemental C-SCRM Guidance: The organization should incorporate C-SCRM activities when media is
3936 　　　transported, either by organizational or non-organizational personnel. Some of the techniques to protect
3937 　　　media during transport and storage include cryptographic techniques and approved custodian services.
3938
3939 　　　Level(s): 1, 2

3940 **MP-6　MEDIA SANITIZATION**

3941        Supplemental C-SCRM Guidance: Organizations should specify and include in agreements (e.g.,
3942        contracting language) media sanitization policies for their suppliers, developers, system integrators,
3943        external system service providers, and other ICT/OT-related service providers. Media is used throughout
3944        the SDLC. Media traversing or residing in the cyber supply chain may originate anywhere including from
3945        suppliers, developers, system integrators, external system service providers, and other ICT/OT-related
3946        service providers. It can be new, refurbished, or reused. Media sanitization is critical to ensure that
3947        information is removed before the media is used, reused, or discarded. For media containing privacy or
3948        other sensitive information (e.g. CUI), the organization should require its prime contractors to implement
3949        this control and flow down this requirement to relevant sub-tier contractors.

3950        Level(s): 2, 3
3951
3952        Related Controls: MP-6(1), MP-6(2), MP-6(3), MP-6(7), MP-6(8)
3953

**FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION**

FIPS 200 specifies the Physical and Environmental Protection minimum security requirement as follows:

> *Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.*

Cyber supply chains span the physical and logical world. Physical factors include, for example, weather and road conditions that may have an impact on transporting cyber components (or devices) from one location to another between persons or organizations within a supply chain. If not properly addressed as a part of the C-SCRM risk management processes, physical and environmental risks may have a negative impact on the organization's ability to receive critical components in a timely manner, which may in turn impact their ability to perform mission operations. Organizations should require implementation of appropriate physical and environmental control within their supply chain.

**PE-1    POLICY AND PROCEDURES**

Supplemental C-SCRM Guidance: The organization should integrate C-SCRM practices and requirements into physical and environmental protection policy and procedures. The degree of protection should be commensurate with the degree of integration. The physical and environmental protection policy should ensure that the physical interfaces of the cyber supply chain have adequate protection and audit for such protection.

Level(s): 1, 2, 3

**PE-2    PHYSICAL ACCESS AUTHORIZATIONS**

Supplemental C-SCRM Guidance: Organizations should ensure only authorized individuals with a need for physical access have access to information or systems (e.g., sensitive or classified). Such authorizations should specify what the individual is permitted or not permitted to do with regard to their physical access (e.g. view, alter/configure, insert something, connect something, remove, etc.). Agreements should address physical access authorization requirements and the organization should require its prime contractors to implement this control, flowing down this requirement to relevant sub-tier contractors. Authorization for non-Federal employees should follow an approved protocol, which includes documentation of the authorization, to include specifying any prerequisites or constraints that pertain to such authorization (e.g., individual must be escorted by a Federal employee, individual must be badged, individual is permitted physical access during normal business hours, etc.).

Level(s): 2, 3

Control Enhancement(s):

**(1)** *PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION OR ROLE*

Supplemental C-SCRM Guidance: Role-based authorizations for physical access should include federal (e.g., agency/department employees) and non-federal employees (e.g., suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers). When role-based authorization is used, the type and level of access allowed for that role or position must be pre-established and documented.

Level(s): 2, 3

**PE-3　PHYSICAL ACCESS CONTROL**

Supplemental C-SCRM Guidance: Physical access control should include individuals and organizations engaged in the organization's cyber supply chain. A vetting process should be in place based on organizational-defined requirements and policy prior to granting access to the cyber supply chain infrastructure and any relevant elements. Access establishment, maintenance, and revocation processes should meet organizational access control policy rigor. The speed of revocation for suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers needing access to physical facilities should be managed in accordance with the activities performed in their contracts. Prompt revocation is critical when either individual or organizational need no longer exists.

Level(s): 2, 3

Control Enhancement(s):

**(1)** *PHYSICAL ACCESS CONTROL | SYSTEM ACCESS*

Supplemental C-SCRM Guidance: Physical access controls should be extended to contractor personnel. Any contractor resources providing services support with physical access to the cyber supply chain infrastructure and any relevant elements should adhere to access controls. Policies and procedures should be consistent with those applied to employee personnel with similar levels of physical access.

Level(s): 2, 3

**(2)** *PHYSICAL ACCESS CONTROL | FACILITY AND SYSTEMS*

Supplemental C-SCRM Guidance: When determining the extent, frequency, and/or randomness of facility security checks of facilities, organizations should account for exfiltration risks resulting from covert listening devices. Such devices may include wiretaps, roving bugs, cell site simulators, and other eavesdropping technologies that can transfer sensitive information out of organizations.

Level(s): 2, 3

**(5)** *PHYSICAL ACCESS CONTROL | TAMPER PROTECTION*

Supplemental C-SCRM Guidance: Tamper protection is critical for reducing cyber supply chain risks in products. The organization should implement validated tamper protections techniques within the cyber supply chain. For critical products, the organization should require and assess whether and to what extent a supplier has implemented tamper protection mechanism. The assessment may also include whether and how such mechanisms are required and applied by the supplier's upstream supply chain entities.

Level(s): 2, 3

**PE-6　MONITORING PHYSICAL ACCESS**

Supplemental C-SCRM Guidance: Individuals physically accessing the organization's facilities, information, or physical asset(s), including via the cyber supply chain, may be employed by the organization's employees, on-site or remotely located contractors, visitors, other third parties (e.g., maintenance personnel under contract with the contractor organization), or an individual affiliated with an organization in the upstream supply chain.  The organization should monitor these individuals' activities to reduce associated cyber supply chain risks or require monitoring in agreements.

Level(s): 1, 2, 3

## PE-16   DELIVERY AND REMOVAL

Supplemental C-SCRM Guidance: This control enhancement reduces cyber supply chain risks introduced during the physical delivery and removal of hardware components from the organization's information systems or cyber supply chain.

Level(s): 3

## PE-17   ALTERNATE WORK SITE

Supplemental C-SCRM Guidance: The organization should incorporate protections to guard against cyber supply chain risks associated with organizational employees or contractor personnel within or accessing the supply chain infrastructure using alternate work sites. This can include third party personnel who may also work from alternate worksites.

Level(s): 3

## PE-18   LOCATION OF SYSTEM COMPONENTS

Supplemental C-SCRM Guidance: Physical and environmental hazards or disruptions have an impact on the availability of products that are or will be acquired and physically transported to the organization's locations. For example, organizations should incorporate the manufacturing, warehousing, or distribution location of information system components critical for agency operations when planning for alternative suppliers for these components.

Level(s): 1, 2, 3

Related Controls: CP-6, CP-7

## PE-20   ASSET MONITORING AND TRACKING

Supplemental C-SCRM Guidance: The organization should, whenever possible and practical, use asset location technologies to track system and components transported between entities across the supply chain, between protected areas, or in storage awaiting implementation, testing, maintenance, or disposal. Methods include RFID,  digital signatures, or blockchains. These technologies help protect against:

   a.   Diverting system or component for counterfeit replacement;
   b.   Loss of confidentiality, integrity, or availability of system or component function and data (including data contained within the component and data about the component); and
   c.   Interrupting supply chain and logistics processes for critical components. In addition to providing protection capabilities, asset location technologies also help gather data that can be used for incident management.

Level(s): 2, 3

4089    **PE-23   FACILITY LOCATION**

4090    Supplemental ICT SCRM Guidance: Organizations should incorporate Facility Location when assessing
4091    risk associated with suppliers. Factors may include geographic location (e.g., Continental United States
4092    (CONUS), Outside the Continental United States (OCONUS)), physical protections in place at one or more
4093    of the relevant facilities, local management and control of such facilities, environmental hazard potential
4094    (e.g., Located in a high risk seismic zone), and alternative facility locations.  For critical vendors or
4095    products, organizations should specifically address any requirements or restrictions concerning the vendors
4096    (or their upstream supply chain providers) facility locations in contracts and flow down this requirement to
4097    relevant sub-level contractors.
4098
4099    Level(s): 2, 3
4100
4101    Related Controls: SA-9(8)
4102
4103
4104

4105
4106
4107

4108    **FAMILY: PLANNING**
4109
4110    FIPS 200 specifies the Planning minimum security requirement as follows:
4111
4112        *Organizations must develop, document, periodically update, and implement security*
4113        *plans for organizational information systems that describe the security controls in*
4114        *place or planned for the information systems and the rules of behavior for individuals*
4115        *accessing the information systems.*
4116
4117    C-SCRM should influence security planning, including such activities as security architecture,
4118    coordination with other organizational entities, and development of System Security Plans.
4119    When acquiring products and services from suppliers, developers, system integrators, external
4120    system service providers, and other ICT/OT-related service providers, organizations may be
4121    sharing facilities with those organizations, have employees of these entities on the organization's
4122    premises, or use information systems that belong to those entities. In these and other applicable
4123    situations, organizations should coordinate their security planning activities with these entities to
4124    ensure appropriate protection of an organization's processes, information systems, as well as of
4125    the systems and components traversing the cyber supply chain. When establishing security
4126    architectures, organizations should provide for component and supplier diversity to manage the
4127    cyber supply chain risks to include suppliers going out of business or stopping the production of
4128    specific components. Finally, as stated in Section 2 and Appendix C, organizations should
4129    integrate C-SCRM controls into their Risk Response Frameworks (Levels 1 and 2) as well as C-
4130    SCRM Plans (Level 3).
4131

4132    **PL-1    POLICY AND PROCEDURES**

4133        Supplemental C-SCRM Guidance: Security planning policy and procedures should integrate C-SCRM.
4134        This includes creating, disseminating, and updating security policy, operational policy, and procedures for
4135        C-SCRM to shape acquisition or development requirements and the follow-on implementation, operations,
4136        and maintenance of systems and system interfaces and network connections. The C-SCRM policy and
4137        procedures provide inputs into and take guidance from C-SCRM Strategy & Implementation Plan at Level
4138        1.  The C-SCRM policy and procedures provide guidance to and take inputs from System Security Plan and
4139        C-SCRM Plan at Level 3.  In Level 3, ensure that the full SDLC is covered from the C-SCRM perspective.
4140
4141        Level(s): 2
4142
4143        Related Controls: PL-2, PM-30

4144    **PL-2    SYSTEM SECURITY AND PRIVACY PLANS**

4145        Supplemental C-SCRM Guidance: The system security plan (SSP) should integrate C-SCRM. The
4146        organization may choose to develop a stand-alone C-SCRM plan for an individual system or integrate
4147        SCRM controls into their SSP. The system security plan and/or system-level C-SCRM plan provide inputs
4148        into and take guidance from the C-SCRM Strategy & Implementation Plan at Level 1 and C-SCRM policy
4149        at Levels 1 and 2.  In addition to coordinating within the organization, the organization should coordinate
4150        with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related
4151        service providers to develop and maintain their SSPs. For example, building and operating a system
4152        requires a significant amount of coordination and collaboration between the organization and system
4153        integrator personnel. Such coordination and collaboration should be addressed in the system security plan

or stand-alone C-SCRM plan. These plans should also take into account that suppliers or external service providers may not be able to customize to the acquirer's requirements. It is recommended that suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers also develop C-SCRM plans for non-federal (i.e., contractor) systems that are processing federal agency information, and flow down this requirement to relevant sub-level contractors.

Section 2, Appendix C, and Appendix D provide guidance on C-SCRM strategy, policy, and plan. Controls in this publication (NIST SP 800-161 Rev. 1) should be used for the C-SCRM portion of the SSP.

Level(s): 3

Related Controls: PM-30

## PL-4    RULES OF BEHAVIOR

Supplemental C-SCRM Guidance: Rules of behavior apply to contractor personnel as well as to internal agency personnel. Contractor organizations are responsible for ensuring that their employees follow applicable rules of behavior. Individual contractors should not be granted access to agency systems or data until they have acknowledged and demonstrated compliance with this control. Failure to meet this control can result in removal of access for such individuals.

Level(s): 2, 3

## PL-7    CONCEPT OF OPERATIONS

Supplemental C-SCRM Guidance:  Concept of operations (CONOPS) should describe how the organization intends to operate the system from the perspective of C-SCRM. It should integrate C-SCRM and be managed and updated throughout the SDLC to address cyber supply chain risks to the applicable system.

Level(s): 3

## PL-8    SECURITY AND PRIVACY ARCHITECTURES

Supplemental C-SCRM Guidance: Security and privacy architecture defines and directs implementation of security and privacy-protection methods, mechanisms, and capabilities to the underlying systems and networks, as well as the information system that is being created. Security architecture is fundamental to C-SCRM because it helps to ensure security is built-in throughout the SDLC. Organizations should consider implementing zero-trust architectures. organization should also ensure that the security architecture is well understood by system developers/engineers and system security engineers. This control applies to both federal agency and non-federal agency employees.

Level(s): 2, 3

Control Enhancement(s):

**(2)**   *SECURITY AND PRIVACY ARCHITECTURES | SUPPLIER DIVERSITY*

Supplemental C-SCRM Guidance: Supplier diversity provides options for addressing information security and cyber supply chain concerns. The organization should incorporate this control as it relates to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

4200    The organization should plan for potential replacement of suppliers, developers, system integrators,
4201    external system service providers, and other ICT/OT-related service providers in case one is no longer
4202    able to meet the organization's requirements (e.g., company goes out of business or does not meet
4203    contractual obligations).
4204
4205    Incorporate supplier diversity for off-the-shelf (commercial or government) components during
4206    acquisition security assessments. Evaluation of alternatives should include, for example, feature parity,
4207    interoperability, commodity components, and ability to provide multiple delivery paths.
4208
4209    Level(s): 2, 3
4210

4211    **PL-9    CENTRAL MANAGEMENT**

4212    Supplemental C-SCRM Guidance: C-SCRM controls are managed centrally at Level 1 through C-
4213    SCRM Strategy & Implementation Plan, and at Levels 1 and 2 through C-SCRM Policy. C-SCRM
4214    PMO described in Section 2, centrally manages C-SCRM controls at those two Levels.  At Level 3, C-
4215    SCRM controls are managed on an information system basis though SSP and/or C-SCRM Plan.
4216
4217    Level(s): 1, 2
4218

4219    **PL-10    BASELINE SELECTION**

4220    Supplemental C-SCRM Guidance: Organizations should include C-SCRM controls in their control
4221    baselines. Organizations should identify and select C-SCRM controls based on C-SCRM requirements
4222    identified within each of the levels. A C-SCRM PMO may assist in identifying C-SCRM control
4223    baselines that meet common C-SCRM requirements for different groups, communities of interest, or
4224    the organization as a whole.
4225
4226    Level(s): 1, 2

**FAMILY: PROGRAM MANAGEMENT**

FIPS 200 does not specify Program Management minimum security requirements.

NIST SP 800-53 Rev. 5 states that "the program management controls … are implemented at the organization level and not directed at individual information systems." Those controls apply to the entire organization (i.e., federal agency) and support the organization's overarching information security program. Program management controls support and provide inputs and feedback to organization-wide C-SCRM activities.

All Program Management controls should be applied in a C-SCRM context. Within federal agencies the C-SCRM PMO function or a similar is responsible for implementing Program Management controls. Section 3 provides guidance on C-SCRM PMO and its functions and responsibilities.

**PM-2    INFORMATION SECURITY PROGRAM LEADERSHIP ROLE**

Supplemental C-SCRM Guidance: Senior information security officer (e.g., CISO) and senior agency official responsible for acquisition (e.g., Chief Acquisition Officer (CAO) or Senior Procurement Executive (SPE)) have key responsibilities for C-SCRM and the overall cross-organizational coordination and collaboration with other applicable senior personnel within the organization such as the CIO, the head of facilities/physical security, and the risk executive (function).   This coordination should occur regardless of specific department and agency organizational structure and specific titles of relevant senior personnel. The coordination could be executed by C-SCRM PMO or another similar function.  Section 2 provides more guidance on C-SCRM roles and responsibilities.

Level(s): 1, 2

**PM-3    INFORMATION SECURITY AND PRIVACY RESOURCES**

Supplemental C-SCRM Guidance: An organization's C-SCRM program- requires dedicated, sustained funding and human resources to successfully implement agency C-SCRM requirements.  Section 3 of this document provides guidance on dedicated funding for C-SCRM programs.  The organization should also ensure that C-SCRM requirements are integrated into major IT investments to ensure that the funding is appropriately allocated through the capital planning and investment request process. For example, should an RFID infrastructure be required to improve C-SCRM to secure and improve inventory or logistics management efficiency of the organization's supply chain, appropriate IT investments are likely required to ensure successful planning and implementation. Other examples include any investment into the development or test environment for critical components. In such a case, funding and resources are needed to acquire and maintain appropriate information systems, networks, and components to meet specific C-SCRM requirements that support the mission.

Level(s): 1, 2

**PM-4    PLAN OF ACTION AND MILESTONES PROCESS**

Supplemental C-SCRM Guidance: C-SCRM items should be included in the POA&M at all levels.

Level(s): 2, 3

4273     Related Controls: CA-5, PM-30
4274

4275     **PM-5     SYSTEM INVENTORY**

4276     Supplemental C-SCRM Guidance: Having a current system inventory is foundational for C-SCRM.  Not
4277     having a system inventory may lead to organization's inability to identify system and supplier criticality
4278     which will result in inability to conduct C-SCRM activities.  To ensure that all applicable suppliers are
4279     identified and categorized for criticality, organizations should include relevant supplier information in the
4280     system inventory and maintain its currency and accuracy.
4281
4282     Level(s): 2, 3
4283

4284     **PM-6     MEASURES OF PERFORMANCE**

4285     Supplemental C-SCRM Guidance: Organizations should use measures of performance to track
4286     implementation, efficiency, effectiveness, and impact of C-SCRM activities.  C-SCRM PMO is responsible
4287     for creating C-SCRM measures of performance in collaboration with other applicable stakeholders to
4288     include identifying appropriate audience and decision makers and providing guidance on data collection,
4289     analysis, and reporting.
4290
4291     Level(s): 1, 2

4292

4293     **PM-7     ENTERPRISE ARCHITECTURE**

4294     Supplemental C-SCRM Guidance: C-SCRM should be integrated when designing and maintaining
4295     enterprise architecture.
4296
4297     Level(s): 1, 2

4298

4299     **PM-8     CRITICAL INFRASTRUCTURE PLAN**

4300     Supplemental C-SCRM Guidance: C-SCRM should be integrated when developing and maintaining critical
4301     infrastructure plan.
4302
4303     Level(s): 1
4304

4305     **PM-9     RISK MANAGEMENT STRATEGY**

4306     Supplemental C-SCRM Guidance: Risk management strategy should address cyber supply chain risks.
4307     Section 2, Appendix C, and Appendix D of this document provide guidance on integrating C-SCRM into
4308     Risk Management Strategy.
4309
4310     Level(s): 1
4311

4312     **PM-10  AUTHORIZATION PROCESS**

4313        Supplemental C-SCRM Guidance: C-SCRM should be integrated when designing and implementing
4314        authorization processes.
4315
4316        Level(s): 1, 2
4317

4318   **PM-11   MISSION AND BUSINESS PROCESS DEFINITION**

4319        Supplemental C-SCRM Guidance: Organization's mission and business processes should address cyber
4320        supply chain risks.  When addressing mission/business process definitions, the organization should ensure
4321        that C-SCRM activities are incorporated into the support processes for achieving mission success. For
4322        example, a system supporting a critical mission function that has been designed and implemented for easy
4323        removal and replacement should a component fail may require the use of somewhat unreliable hardware
4324        components. A C-SCRM activity may need to be defined to ensure that the supplier makes component
4325        spare parts readily available if replacement is needed.
4326
4327        Level(s): 1, 2, 3
4328

4329   **PM-12   INSIDER THREAT PROGRAM**

4330        Supplemental C-SCRM Guidance: An insider threat program should include C-SCRM and be tailored for
4331        both federal and non-federal agency individuals who have access to agency systems and networks.  This
4332        control applies to contractors and subcontractors and should be implemented throughout the SDLC.
4333
4334        Level(s): 1, 2, 3

4335

4336   **PM-13   SECURITY AND PRIVACY WORKFORCE**

4337        Supplemental C-SCRM Guidance: Security and privacy workforce development and improvement should
4338        ensure that relevant C-SCRM topics are integrated into the content and initiatives produced by the program.
4339        Section 2 provides information on C-SCRM roles and responsibilities. NIST SP 800-161 can be used as a
4340        source of topics and activities to include in the security and privacy workforce program.
4341
4342        Level(s): 1, 2
4343

4344   **PM-14   TESTING, TRAINING, AND MONITORING**

4345        Supplemental C-SCRM Guidance: Organization's testing, training, and monitoring processes should
4346        include C-SCRM activities.  C-SCRM PMO can provide guidance and support on how to integrate C-
4347        SCRM into testing, training, and monitoring plans.
4348
4349        Level(s): 1, 2
4350

4351   **PM-15   SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS**

4352        Supplemental C-SCRM Guidance: Contact with security and privacy groups and associations should
4353        include C-SCRM practitioners and those with C-SCRM responsibilities.  Acquisition, legal, critical
4354        infrastructure, and supply chain groups and associations should be incorporated.  C-SCRM PMO can help

identify agency personnel who could benefit from participation, specific groups to participate in, and relevant topics.

Level(s): 1, 2

**PM-16   THREAT AWARENESS PROGRAM**

Supplemental C-SCRM Guidance: Threat awareness program should include threats emanating from the supply chain.  When addressing supply chain threat awareness, knowledge should be shared between stakeholders within the boundaries of the organization's information sharing policy. C-SCRM PMO can help identify C-SCRM stakeholders to include in threat information sharing, as well as potential sources of information for supply chain threats.

Level(s): 1, 2

**PM-17   PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS**

Supplemental C-SCRM Guidance: Policy and procedures for controlled unclassified information (CUI) on external systems should include protecting relevant cyber supply chain information.  Conversely, it should include protecting agency information residing in external systems, because such external systems are part of agency supply chain.

Level(s): 2

**PM-18   PRIVACY PROGRAM PLAN**

Supplemental C-SCRM Guidance: Privacy Program Plan should include C-SCRM. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 1, 2

**PM-19   PRIVACY PROGRAM LEADERSHIP ROLE**

Supplemental C-SCRM Guidance: Privacy program leadership role should be included is a stakeholder in applicable C-SCRM initiatives and activities.

Level(s): 1

**PM-20   DISSEMINATION OF PRIVACY PROGRAM INFORMATION**

Supplemental C-SCRM Guidance: Dissemination of privacy program information should be protected from cyber supply chain risks.

Level(s): 1, 2

**PM-21   ACCOUNTING OF DISCLOSURES**

4397  Supplemental C-SCRM Guidance: Accounting of disclosures should be protected from cyber supply chain
4398  risks.
4399
4400  Level(s): 1, 2
4401

4402  **PM-22  PERSONALLY IDENTIFIABLE INFORMATION QUALITY MANAGEMENT**

4403  Supplemental C-SCRM Guidance: Personally identifiable information (PII) quality management should
4404  take into account and manage cyber supply chain risks to this information.
4405
4406  Level(s): 1, 2
4407

4408  **PM-23  DATA GOVERNANCE BODY**

4409  Supplemental C-SCRM Guidance: Data governance body is a stakeholder in C-SCRM and as such should
4410  be included in cross-agency collaboration and information sharing of C-SCRM activities and initiatives
4411  (e.g., by participating in inter-agency bodies such as the FASC).
4412
4413  Level(s): 1
4414

4415  **PM-25  MINIMIZATION OF PERSONALLY IDENTIFIABLE INFORMATION USED IN TESTING,**
4416  **TRAINING, AND RESEARCH**

4417  Supplemental C-SCRM Guidance: Cyber supply chain risks to personally identifiable information should
4418  be addressed by minimization policies and procedures described in this control.
4419
4420  Level(s): 2
4421

4422  **PM-26  COMPLAINT MANAGEMENT**

4423  Supplemental C-SCRM Guidance: Complaint management process and mechanisms should be protected
4424  from cyber supply chain risks. Organizations should also integrate C-SCRM security and privacy controls
4425  when fielding complaints from vendors or the general public (e.g., departments and agencies fielding
4426  inquiries related to exclusions and removals).
4427
4428  Level(s): 2, 3
4429

4430  **PM-27  PRIVACY REPORTING**

4431  Supplemental C-SCRM Guidance: Privacy reporting process and mechanisms should be protected from
4432  cyber supply chain risks.
4433
4434  Level(s): 2, 3
4435

4436  **PM-28  RISK FRAMING**

4437  Supplemental C-SCRM Guidance: C-SCRM should be included in risk framing.  Section 2 and Appendix
4438  C provide detail guidance on integrating C-SCRM into risk framing.

4439
4440      Level(s): 1
4441


4442   **PM-29   RISK MANAGEMENT PROGRAM LEADERSHIP ROLES**

4443      Supplemental C-SCRM Guidance: Risk management program leadership roles should include C-SCRM
4444      responsibilities and be included in C-SCRM collaboration across the organization.  Section 2 and Appendix
4445      C provide detail guidance C-SCRM roles and responsibilities.
4446
4447      Level(s): 1
4448


4449   **PM-30   SUPPLY CHAIN RISK MANAGEMENT STRATEGY**

4450      Supplemental C-SCRM Guidance: Supply Chain Risk Management Strategy (also known as C-SCRM
4451      Strategy) should be complemented with a C-SCRM Implementation Plan that lays out detailed initiatives
4452      and activities for the organization with timelines and responsible parties.  This implementation plan can be
4453      a POA&M or be included in a POA&M.  Based on the C-SCRM Strategy and Implementation Plan at
4454      Level 1, the organization should select and document common C- SCRM controls that need to address the
4455      organization, program, and system-specific needs.  These controls should be iteratively integrated the C-
4456      SCRM Policy at Levels 1 and 2, and C-SCRM Plan (or SSP if required) at Level 3.  See Section 2 and
4457      Appendix C for further guidance on risk management.
4458
4459      Level(s): 1, 2
4460
4461      Related Controls: PL-2


4462   **PM-31   CONTINUOUS MONITORING STRATEGY**

4463      Supplemental C-SCRM Guidance: Continuous monitoring strategy and program should integrate C-SCRM
4464      controls at Levels 1, 2, and 3 in accordance with Supply Chain Risk Management Strategy.
4465
4466      Level(s): 1, 2, 3
4467
4468      Related Controls: PM-30
4469


4470   **PM-32   PURPOSING**

4471      Supplemental C-SCRM Guidance: Extending systems assigned to support specific mission or business
4472      functions beyond their initial purpose subjects those systems to unintentional risks to include cyber supply
4473      chain risks.  Application of this control should include explicit incorporation of cyber supply chain
4474      exposures.
4475
4476      Level(s): 2, 3
4477
4478

4479
4480   **FAMILY: PERSONNEL SECURITY**
4481
4482   FIPS 200 specifies the Personnel Security minimum security requirement as follows:
4483
4484       *Organizations must: (i) ensure that individuals occupying positions of responsibility*
4485       *within organizations (including third-party service providers) are trustworthy and meet*
4486       *established security criteria for those positions; (ii) ensure that organizational*
4487       *information and information systems are protected during and after personnel actions*
4488       *such as terminations and transfers; and (iii) employ formal sanctions for personnel*
4489       *failing to comply with organizational security policies and procedures.*
4490
4491   Personnel that have access to an organization's cyber supply chain should be covered by the
4492   organization's personnel security controls. These personnel include acquisition and contracting
4493   professionals, program managers, supply chain and logistics professionals, shipping and
4494   receiving staff, information technology professionals, quality professionals, mission and business
4495   owners, system owners, and information security engineers. Organizations should also work with
4496   suppliers, developers, system integrators, external system service providers, and other ICT/OT-
4497   related service providers to ensure they apply appropriate personnel security controls to the
4498   personnel that interact with the organization's supply chain, as appropriate.
4499

4500   **PS-1      POLICY AND PROCEDURES**

4501       <u>Supplemental C-SCRM Guidance</u>: At each level, personnel security policy and procedures, and related C-
4502       SCRM Strategy/Implementation Plan, C-SCRM Policies, and C-SCRM Plan(s) need to define the roles for
4503       the personnel who are engaged in the acquisition, management, and execution of supply chain security
4504       activities. These roles also need to state acquirer personnel responsibilities with regards to relationships
4505       with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related
4506       service providers. Policies and procedures need to consider the full system development life cycle of
4507       systems and the roles and responsibilities needed to address the various supply chain infrastructure
4508       activities.
4509
4510       Level 1: Applicable roles include risk executive, CIO, CISO, contracting, logistics, delivery/receiving,
4511       acquisition security, and other functions providing supporting supply chain activities.
4512
4513       Level 2: Applicable roles include program executive and individuals (e.g., non-federal employees including
4514       contractors) within the acquirer organization responsible for program success (e.g., Program Manager and
4515       other individuals).
4516
4517       Level 3: Applicable roles include system engineers or system security engineers throughout the operational
4518       system life cycle from requirements definition, development, test, deployment, maintenance, updates,
4519       replacements, delivery/receiving, and IT.
4520
4521       Roles for supplier, developer, system integrator, external system service provider, and other ICT/OT-
4522       related service provider personnel responsible for the success of the program should be noted in an
4523       agreement between acquirer and these parties (e.g., contract).
4524
4525       The organization should require its prime contractors to implement this control and flow down this
4526       requirement to relevant sub-tier contractors.
4527

4528
4529        Level(s): 1, 2, 3
4530
4531        Related Control(s): SA-4

4532  **PS-3    PERSONNEL SCREENING**

4533        Supplemental C-SCRM Guidance: To mitigate insider threat risks, personnel screening policies and
4534        procedures should be extended to any contractor personnel with authorized access to information systems,
4535        system components, or information system services. Continuous monitoring activities should be
4536        commensurate with the contractor's level of access to sensitive, classified, or regulated information and
4537        should be consistent with broader organizational policies.  Screening requirements should be incorporated
4538        into agreements and flowdown to sub-tier contractors.
4539
4540        Level(s): 2, 3

4541  **PS-6    ACCESS AGREEMENTS**

4542        Supplemental C-SCRM Guidance: The organization should define and document access agreements for all
4543        contractors or other external personnel that may have a need to access the organization's data, systems, or
4544        network, whether physically or logically. Access agreements should state the appropriate level and method
4545        of access to the information system and supply chain network. Additionally, terms of access should be
4546        consistent with the organization's information security policy and may need to specify additional
4547        restrictions, such as allowing access during specific timeframes, from specific locations, or by only
4548        personnel who have satisfied additional vetting requirements. The organization should deploy audit
4549        mechanisms to review, monitor, update, and track access by these parties in accordance with the access
4550        agreement. As personnel vary over time, the organization should implement a timely and rigorous
4551        personnel security update process for the access agreements.
4552
4553        When information systems and network products and services are provided by an entity within the
4554        organization, there may be an existing access agreement in place. When such an agreement does not exist,
4555        it should be established.
4556
4557        NOTE: While the audit mechanisms may be implemented in Level 3, the agreement process with required
4558        updates should be implemented at Level 2 as a part of program management activities.
4559
4560        The organization should require its prime contractors to implement this control and flow down this
4561        requirement to relevant sub-tier contractors.
4562
4563        Level(s): 2, 3

4564  **PS-7    EXTERNAL PERSONNEL SECURITY**

4565        Supplemental C-SCRM Guidance: Third-party personnel that have access to organization's information
4566        systems and networks must meet the same personnel security requirements as organizational personnel.
4567        Examples of such third-party personnel can include the system integrator, developer, supplier, or external
4568        service provider used for delivery, contractors or service providers that are using the ICT/OT systems, or
4569        supplier maintenance personnel brought in to address component technical issues not solvable by the
4570        organization or system integrator.
4571
4572        Level(s): 2
4573

**FAMILY: PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND
TRANSPARENCY**

Personally identifiable information processing and transparency is a new control family,
developed specifically to address PII processing and transparency concerns.

The organization should keep in mind that some suppliers have comprehensive security and
privacy practices and systems that may go above and beyond the organization's requirements.
The organizations should work with suppliers to understand the extent of their privacy practices
and how they meet the organization's needs.

**PT-1     POLICY AND PROCEDURES**

Supplemental C-SCRM Guidance: Organizations should ensure that supply chain concerns are included in
PII processing and transparency policies and procedures, and related C-SCRM Strategy/Implementation
Plan, C-SCRM Policies, and C-SCRM Plan.  The policy can be included as part of the general security and
privacy policy or can be represented by multiple policies.

The procedures can be established for the security and privacy program in general and individual
information systems. These policy and procedures should address purpose, scope, roles, responsibilities,
management commitment, coordination among organizational entities, and privacy compliance to support
systems/components within information systems or the supply chain.

Policies and procedures need to be in place to ensure contracts state what PII data will be shared, which
contractor personnel may have access to the PII, controls protecting PII, and how long it can be kept and
what happens to it at the end of a contract.
a.   When working with a new supplier, ensure that the agreement includes the most recent set of
     applicable security requirement.

Contractors need to abide by relevant laws and policies regarding information (PII and other sensitive
information)

The organization should require its prime contractors to implement this control and flow down this
requirement to relevant sub-tier contractors.


Level(s): 1, 2, 3

**FAMILY: RISK ASSESSMENT**

FIPS 200 specifies the Risk Assessment minimum security requirement as follows:

> *Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operating of organizational information systems and the associated processing, storage, or transmission of organizational information.*

NIST SP 800-161 Rev. 1 provides guidance for managing an organization's cyber supply chain risks and expands this control to integrate cyber supply chain risk assessment activities, as described in *Section 2* and *Appendix C*.

**RA-1    POLICY AND PROCEDURES**

Supplemental C-SCRM Guidance: Risk assessments should be performed at the enterprise, mission/program, and operational levels of the organization. The system-level risk assessment should include both the cyber supply chain infrastructure (e.g., development and testing environments, and delivery systems) and the information system/components traversing the cyber supply chain. System-level risk assessments significantly intersect with the SDLC and should complement the organizations broader RMF activities which take part during the SDLC. A criticality analysis will ensure that mission-critical functions and components are given higher priority due to their impact to the mission, if compromised. The policy should include cyber supply chain-relevant roles applicable to performing and coordinating risk assessments across the organization (see Section 2 for the listing and description of roles). Applicable roles within suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers should be defined.

Level(s): 1, 2, 3

**RA-2    SECURITY CATEGORIZATION**

Supplemental C-SCRM Guidance: Security categorization is critical to C-SCRM at Levels 1, 2, and 3. In addition to FIPS 199 categorization, for C-SCRM, security categorization should be based on the criticality analysis which is performed as part of the SDLC. See Section 2 and NISTIR 8179 for a detailed description of criticality analysis.

Level(s): 1, 2, 3

Related Controls: RA-9

**RA-3    RISK ASSESSMENT**

Supplemental C-SCRM Guidance: Risk assessments should include an analysis of criticality, threats, vulnerabilities, likelihood, and impact, as described in detail in Appendix C, *C-SCRM Activities in the Risk Management Process*. Data to be reviewed and collected includes C-SCRM-specific roles, processes, and results of system/component and services acquisitions, implementation, and integration. Risk assessments should be performed at Levels 1, 2, and 3. Risk assessments at higher levels should consist primarily of a synthesis of various risk assessments performed at lower levels and used for understanding the overall impact with the Level (e.g., at the organization or mission/function levels). C-SCRM risk assessments should complement and inform risk assessments which are performed as ongoing activities throughout the SDLC and processes should be appropriately aligned to or integrated into ERM processes and governance.

Level(s): 1, 2, 3

Related Control(s): RA-3(1)

**RA-5    VULNERABILITY MONITORING AND SCANNING**

Supplemental C-SCRM Guidance: Vulnerability monitoring should cover suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers in the organization's supply chain. This includes employing data collection tools to maintain a continuous state of awareness about potential vulnerability to suppliers as well as the information systems/ system components/ and raw inputs they provide through the cyber supply chain. Vulnerability monitoring activities should take place at all three levels of the organization. Scoping vulnerability monitoring activities requires organizations to consider suppliers as well as their sub-suppliers. Organizations should consider use of the *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks* outlined in NISTIR 8272 to track and maintain visibility into the relevant components within their supply chain.

Level(s): 2, 3

Control Enhancement(s):

**(3)** *VULNERABILITY MONITORING AND SCANNING | BREADTH AND DEPTH OF COVERAGE*

Supplemental C-SCRM Guidance: Organizations monitoring the cyber supply chain for vulnerabilities should express breadth of monitoring based on the criticality and/or risk profile of the supplier or product/component, and the depth of monitoring based on the level of the supply chain monitoring takes place at (e.g., sub-supplier). Where possible – a component inventory (e.g., hardware, software) may aid organizations in capturing the breadth and depth of the products/components within their cyber supply chain that may need to be monitored and scanned for vulnerabilities.

Level(s): 2, 3

**(6)** *VULNERABILITY MONITORING AND SCANNING | AUTOMATED TREND ANALYSIS*

Supplemental C-SCRM Guidance: Organizations should track trends, over time, in vulnerability to components within the cyber supply chain. This information may help organizations develop procurement strategies that reduce risk exposure density within the supply chain.

Level(s): 2, 3

**RA-7    RISK RESPONSE**

4694    Supplemental C-SCRM Guidance: Organizations should integrate cyber supply chain risk response
4695    capabilities into the overall organization's response posture, ensuring these responses are aligned to and fall
4696    within the boundaries of the organization's tolerance for risk. Risk Response should include consideration
4697    of risk response identification, evaluation of alternatives, and risk response decision activities.
4698
4699    Level(s): 1, 2, 3

4700 **RA-9** **CRITICALITY ANALYSIS**

4701    Supplemental C-SCRM Guidance: Organizations should complete a criticality analysis as a prerequisite
4702    input to cyber supply chain risk assessment activities. First, organizations complete a criticality analysis as
4703    part of the *Frame* step of the C-SCRM Risk Management Process. Then, findings generated in *Assess* step
4704    activities (e.g., criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies) update
4705    and tailor the criticality analysis. A symbiotic relationship exists between the criticality analysis and other
4706    *Assess* step activities in that they inform and enhance one another. For a high-quality criticality analysis –
4707    organizations should employ it iteratively throughout the SLDC and concurrently across the 3 levels.
4708
4709    Level(s): 1, 2, 3

4710 **RA-10** **THREAT HUNTING**

4711    Supplemental C-SCRM Guidance: C-SCRM Threat Hunting activities should supplement the organizations
4712    internal Threat Hunting activities. As a critical part of the cyber supply chain risk management process –
4713    organizations should actively monitor for threats to their cyber supply chain. This requires a collaborative
4714    effort between C-SCRM and other cyber defense-oriented functions within the organization. Threat hunting
4715    capabilities may also be provided via a shared services organization, especially when an organization lacks
4716    the resources to perform threat hunting activities themselves. Typical activities include information sharing
4717    with peer organizations and actively consuming threat intelligence feeds that flag potential indicators of
4718    increased cyber supply chain risks, such as cyber incidents, mergers and acquisitions, and Foreign
4719    Ownership, Control or Influence (FOCI) that may be of concern. Cyber Supply Chain Threat intelligence
4720    should seek out threats to the organization's suppliers as well as information systems/ system components/
4721    and raw inputs they provide. Intelligence gathered enables organizations to proactively identify and
4722    respond to threats emanating from the supply chain.
4723
4724    Level(s): 1, 2, 3
4725
4726

4727   **FAMILY: SYSTEM AND SERVICES ACQUISITION**
4728
4729   FIPS 200 specifies the System and Services Acquisition minimum security requirement as
4730   follows:
4731
4732       *Organizations must: (i) allocate sufficient resources to adequately protect*
4733       *organizational information systems; (ii) employ system development life cycle*
4734       *processes that incorporate information security considerations; (iii) employ software*
4735       *usage and installation restrictions; and (iv) ensure that third-party providers employ*
4736       *adequate security measures to protect information, applications, and/or services*
4737       *outsourced from the organization.*
4738
4739   Organizations acquire ICT/OT products and services through system and services acquisition.
4740   These controls address the activities of an acquirer, as well as the activities of suppliers,
4741   developers, system integrators, external system service providers, and other ICT/OT-related
4742   service providers and related upstream supply chain relationships. They address both physical
4743   and logical aspects of cyber supply chain security, from detection to SDLC and security
4744   engineering principles. C-SCRM concerns are already prominently addressed in NIST SP 800-
4745   53 Rev. 5. NIST SP 800-161 Rev. 1 adds further detail and refinement to these controls.
4746

4747   **SA-1      POLICY AND PROCEDURES**

4748       <u>Supplemental C-SCRM Guidance</u>:  System and services acquisition policy and procedures should address
4749       C-SCRM throughout the acquisition management life cycle process, to include purchases made via charge
4750       cards.  C-SCRM procurement actions and resultant contracts should include requirements language or
4751       clauses that address which controls are mandatory or desirable and may include implementation
4752       specifications, state what is accepted as evidence that the requirement is satisfied, and how conformance to
4753       requirements will be verified and validated.  C-SCRM should also be included as an evaluation factor.
4754       These applicable procurements should not be limited to only those that are directly related to providing an
4755       ICT/OT product or service; while C-SCRM considerations must be applied to these purchases, C-SCRM
4756       should also be considered for any and all procurements of products or services in which there may be an
4757       unacceptable risk of a supplied product or service contractor compromising the integrity, availability, or
4758       confidentiality of an organization's information.  This initial assessment should occur during the
4759       acquisition planning phase and will be minimally informed by an identification and understanding of the
4760       criticality of the organization's mission functions, its high value assets, and the sensitivity of the
4761       information that may be accessible by the supplied product or service provider.  In addition, organizations
4762       should develop policies and procedures that address supply chain risks that may arise during contract
4763       performance, such as a change of ownership or control of the business or when actionable information is
4764       learned that indicates a supplier or a product is a target of a supply chain threat.  Supply chains evolve
4765       continuously through mergers and acquisitions, joint ventures, and other partnership agreements. The
4766       policy should help organizations understand these changes and use thus obtained information to inform
4767       their C-SCRM activities. Organizations can obtain status of such changes through, for example, monitoring
4768       public announcements about company activities or any communications initiated by suppliers, developers,
4769       system integrators, external system service providers, and other ICT/OT-related service providers. See
4770       Section 3 for further guidance on C-SCRM in the federal acquisition process.
4771
4772       <u>Level(s)</u>: 1, 2, 3

4773   **SA-2      ALLOCATION OF RESOURCES**

4774  Supplemental C-SCRM Guidance: The organization should incorporate C-SCRM requirements when
4775  determining and establishing the allocation of resources.
4776
4777  Level(s): 1, 2

4778  **SA-3    SYSTEM DEVELOPMENT LIFE CYCLE**

4779  Supplemental C-SCRM Guidance: There is a strong relationship between the SDLC and C-SCRM
4780  activities. The organization should ensure that C-SCRM activities integrated into the SDLC for both the
4781  organization and for applicable suppliers, developers, system integrators, external system service providers,
4782  and other ICT/OT-related service providers. In addition to traditional SDLC activities, such as requirements
4783  and design, the SDLC includes activities such as inventory management, acquisition and procurement, and
4784  logical delivery of systems and components. See *Section 2* and *Appendix C* for further guidance on SDLC.
4785
4786  Level(s): 1, 2, 3

4787  **SA-4    ACQUISITION PROCESS**

4788  Supplemental C-SCRM Guidance: Organizations are to include C-SCRM requirements, descriptions, and
4789  criteria in applicable contractual agreements.
4790
4791      a.  Organizations are to establish baseline and tailor-able C-SCRM requirements to apply and
4792          incorporate into contractual agreements when procuring a product or service from suppliers,
4793          developers, system integrators, external system service providers, and other ICT/OT-related
4794          service providers; These include but are not limited to:
4795          1.  C-SCRM requirements that cover regulatory mandates (e.g. prohibition of certain ICT/OT or
4796              suppliers;  address identified and selected controls that are applicable to reducing cyber-
4797              supply chain risk that may be introduced by a procured product or service; and provide
4798              assurance that the contractor is  sufficiently responsible, capable, and trustworthy.
4799          2.  Requirements for critical elements in the supply chain to demonstrate a capability to
4800              remediate emerging vulnerabilities based on open source information and other sources;
4801          3.   Requirements for managing intellectual property ownership and responsibilities for elements
4802              such as software code, data and information, the manufacturing/development/integration
4803              environment, designs, and proprietary processes when provided to the organization for review
4804              or use;
4805          4.  Requirements that  address  the expected life span of the product or system and any
4806              element(s) which may be in a critical path based on their life span, as well as what is required
4807              when end-of-life is near or has been reached.  Organizations should conduct research or solicit
4808              information from bidders or existing providers under contract to understand what end-of-life
4809              options exist (i.e., replace, upgrade, migrate to a new system, etc.).
4810          5.  Articulate any circumstances when secondary market components may be permitted.
4811      b.  Requirements for functional properties, configuration, and implementation information, as well as any
4812          development methods, techniques, or practices which may be relevant; Identify and specify C-SCRM
4813          evaluation criteria, to include weighting of such criteria
4814      c.   Organizations should:
4815          1.   Establish a plan for acquisition of spare parts to ensure adequate supply and execute the plan,
4816              if/when applicable;
4817          2.  Establish a plan for acquisition of alternative sources of supply, as may be necessary during
4818              continuity events or if/when a disruption to the supply chain occurs,
4819      d.  Work with suppliers, developers, system integrators, external system service providers, and other
4820          ICT/OT-related service providers to identify and define existing and acceptable incident response
4821          and information sharing processes, including inputs on vulnerabilities from other organizations
4822          within their supply chains;
4823      e.  Establish and maintain verification procedures and acceptance criteria for delivered products and
4824          services;

4825    f.   Ensure that the continuous monitoring plan includes supply chain aspects in its criteria such as.
4826         including the monitoring of functions/ports/protocols in use. See Section 2 and Appendix C;
4827    g.   Ensure the contract addresses the monitoring of suppliers', developers', system integrators',
4828         external system service providers', and other ICT/OT-related service providers' information
4829         systems located within the supply chain infrastructure. Monitor and evaluate the acquired work
4830         processes and work products where applicable;
4831    h.   Communicate processes for reporting information security weaknesses and vulnerabilities detected
4832         during the use of ICT/OT products or services and ensure reporting to appropriate stakeholders,
4833         including OEMs where relevant;
4834    i.   Review and confirm sustained compliance s with the terms and conditions of the agreement on an
4835         ongoing basis; and
4836
4837    <u>Level(s):</u> 1, 2, 3
4838
4839    <u>Related Controls:</u> SA-4 (1), (2), (3), (6) and (7)
4840
4841    <u>Control Enhancement(s):</u>

4842    **(5)**   *ACQUISITION PROCESS | SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS*

4843          <u>Supplemental C-SCRM Guidance</u>: If an organization needs to purchase components, they need to
4844          ensure that the product specifications are "fit for purpose" and meet the organization's requirements,
4845          whether purchasing directly from the OEM, channel partners, or secondary market.
4846
4847          <u>Level(s):</u> 3

4848    **(7)**   *ACQUISITION PROCESS | NIAP-APPROVED PROTECTION PROFILES*

4849          <u>Supplemental C-SCRM Guidance</u>: This control enhancement requires that the organization build,
4850          procure, and/or use U.S. government protection profile-certified information assurance (IA)
4851          components when possible. NIAP certification can be achieved for OTS (COTS and GOTS).
4852
4853          <u>Level(s):</u> 2, 3
4854

4855    **(8)**   *ACQUISITION PROCESS | CONTINUOUS MONITORING PLAN FOR CONTROLS*

4856          <u>Supplemental C-SCRM Guidance</u>: This control enhancement is relevant to C-SCRM and plans for
4857          continuous monitoring of control effectiveness and should therefore be extended to suppliers,
4858          developers, system integrators, external system service providers, and other ICT/OT-related service
4859          providers.
4860
4861          <u>Level(s):</u> 2, 3

4862    **SA-5    SYSTEM DOCUMENTATION**

4863    <u>Supplemental C-SCRM Guidance</u>: Information system documentation should include relevant C- SCRM
4864    concerns (e.g., C-SCRM plan).
4865
4866    <u>Level(s):</u> 3

4867    **SA-8    SECURITY AND PRIVACY ENGINEERING PRINCIPLES**

4868    <u>Supplemental C-SCRM Guidance</u>: The following security engineering techniques are helpful in managing
4869    cyber supply chain risks:
4870

4871         a.  Anticipate the maximum possible ways that the ICT/OT product or service can be misused and
4872              abused in order to help identify how to protect the product or system from such uses. Address
4873              intended and unintended use scenarios in architecture and design;
4874         b.  Design network and security architectures, systems and components based on the organization's
4875              risk tolerance as determined by risk assessments (see Section 2 and Appendix C);
4876         c.  Document and gain management acceptance and approval for risks that are not fully mitigated;
4877         d.  Limit the number, size, and privilege levels of critical elements; using criticality analysis will aid
4878              in determining which elements or functions are critical. See criticality analysis in Appendix C, and
4879              NISTIR 8179 *Criticality Analysis Process Model: Prioritizing Systems and Components*;
4880         e.  Use security mechanisms that help to reduce opportunities to exploit supply chain vulnerabilities,
4881              including, for example, encryption, access control, identity management, and malware or
4882              tampering discovery;
4883         f.  Design information system components and elements to be difficult to disable (e.g., tamper-
4884              proofing techniques) and, if disabled, trigger notification methods such as audit trails, tamper
4885              evidence, or alarms;
4886         g.  Design delivery mechanisms (e.g., downloads for software) to avoid unnecessary exposure or
4887              access to the cyber supply chain and the systems/components traversing the cyber supply chain
4888              during delivery; and
4889         h.  Design relevant validation mechanisms to be used during implementation and operation.
4890
4891       <u>Level(s):</u> 1, 2, 3

4892   **SA-9**     **EXTERNAL SYSTEM SERVICES**

4893       <u>Supplemental C-SCRM Guidance</u>: C-SCRM supplemental guidance is provided in control enhancements.
4894
4895       <u>Control Enhancement(s):</u>

4896       **(1)** *EXTERNAL SYSTEM SERVICES | RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS*

4897         <u>Supplemental C-SCRM Guidance</u>: See Appendix C - Assess, and Appendices D and E.
4898
4899         <u>Level(s):</u> 2, 3

4900       **(3)** *EXTERNAL SYSTEM SERVICES | ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS*

4901         <u>Supplemental C-SCRM Guidance</u>: Relationships with providers ("providers" within the context of this
4902         enhancement may include suppliers, developers, system integrators, external system service providers,
4903         and other ICT/OT-related service providers) should meet the following supply chain security
4904         requirements:
4905         a.  Requirements definition is complete and reviewed for accuracy and completeness including the
4906              assignment of criticality to various components as well as defining operational concepts and
4907              associated scenarios for intended and unintended use in requirements;
4908         b.  Requirements are based on needs, relevant compliance drivers, criticality analysis, and cyber
4909              supply chain risk assessment;
4910         c.  Cyber-supply chain threats, vulnerabilities, and associated risks are identified and documented;
4911         d.  Organizational data and information integrity, confidentiality, and availability requirements are
4912              defined and shared with the system suppliers, developers, system integrators, external system
4913              service providers, and other ICT/OT-related service providers as appropriate;
4914         e.  Consequences of noncompliance with C-SCRM requirements and information system security
4915              requirements are defined and documented;
4916         f.  Clear delineation of accountabilities, roles, and responsibilities between contractors when multiple
4917              disparate providers are engaged in supporting a system or mission/business function.
4918         g.  Requirements for service contract completion and what defines the end of the suppliers',
4919              developers', system integrators', external system service providers', or other ICT/OT-related

service providers' relationship. This is important to know for re-compete, potential change in provider, and to manage system end-of-life processes.

Level(s): 1, 2, 3

**(4)** *EXTERNAL SYSTEM SERVICES | CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS*

Supplemental C-SCRM Guidance: "Providers" in the context of this enhancement may include suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 3

**(5)** *EXTERNAL SYSTEM SERVICES | PROCESSING, STORAGE, AND SERVICE LOCATION*

Supplemental C-SCRM Guidance: Location may be under the control of the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Organizations should assess C-SCRM risks associated with a given geographic location and apply an appropriate risk response, which may include defining locations that are or are not acceptable and ensuring appropriate protections are in place to address any associated C-SCRM risks.

Level(s): 3

## SA-10   DEVELOPER CONFIGURATION MANAGEMENT

Supplemental C-SCRM Guidance: Developer configuration management is critical for reducing cyber supply chain risks. By conducting configuration management activities, developers reduce occurrence and likelihood of flaws, while increasing accountability and ownership for the changes.  Developer configuration management should be performed both by developers internal to federal agencies and integrators or external service providers.

Level(s): 2, 3

Related Controls: SA-10 (1), (2), (3), (4), (5), and (6)

## SA-11   DEVELOPER TESTING AND EVALUATION

Supplemental C-SCRM Guidance: Depending on the origins of components, this control may be implemented differently. For OTS (off-the-shelf) components, the acquirer should conduct research (e.g., via publicly available resources) or request proof to determine whether the supplier (OEM) has performed such testing as part of their quality/security processes. When the acquirer has control over the application and the development processes, they should require this testing as part of the SDLC. In addition to the specific types of testing activities described in the enhancements, examples of C-SCRM-relevant testing include testing for counterfeits, verifying the origins of components, examining configuration settings prior to integration, and testing interfaces. These types of tests may require significant resources and should be prioritized based on criticality, threat, and vulnerability analyses (described in Section 2 and Appendix C), and the effectiveness of testing techniques. Organizations may also require third-party testing as part of developer security testing.

Level(s): 1, 2, 3

Related Controls: SA-11 (1), (2), (3), (4), (5), (6), (7), (8), and (9)

## SA-15   DEVELOPMENT PROCESS, STANDARDS, AND TOOLS

Supplemental C-SCRM Guidance: Providing documented and formalized development processes to guide internal and system integrator developers is critical to organizations efforts to effectively mitigate cyber supply chain risks. The organization should apply national and international standards and best practices when implementing this control. Using existing standards promotes consistency of implementation, reliable and defendable process, if implemented properly, and interoperability.  The organization's development/maintenance, test, and deployment environments should all be covered by this control. The tools included in this control can be manual or automated. Use of automated tools aids thoroughness, efficiency, and scale of analysis that helps address cyber supply chain risks in the development process. Additionally, the output of such activities and tools provides useful inputs for C-SCRM processes described in Section 2 and Appendix C. This control has applicability to both the internal organization's processes, information systems, and networks as well as applicable system integrators' processes,  systems, and networks.

Level(s): 2, 3

Related Controls: SA-15 enhancements (1), (2), (5), (6), and (7)

Control Enhancement(s):

**(3)** *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | CRITICALITY ANALYSIS*

Supplemental C-SCRM Guidance: This enhancement identifies critical components within the information system. Doing so will help determine the specific C-SCRM activities to be implemented for critical components. See C-SCRM Criticality Analysis described in Appendix C for additional context.

Level(s): 2, 3

**(4)** *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | THREAT MODELING AND VULNERABILITY ANALYSIS*

Supplemental C-SCRM Guidance: This enhancement provides threat modeling/vulnerability analysis for the relevant federal agency and contractor information systems and networks. Performing this analysis will help integrate C-SCRM into code refinement and modification activities. See C-SCRM threat and vulnerability analyses described in Appendix C for additional context.

Level(s): 2, 3

Related Control(s): SA-15(5), SA-15(6), SA-15(7)

**(8)** *DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | REUSE OF THREAT AND VULNERABILITY INFORMATION*

Supplemental C-SCRM Guidance: This enhancement encourages developers to reuse threat and vulnerability information produced by prior development efforts and lessons learned from using the tools to inform ongoing development efforts. Doing so will help determine C-SCRM activities described in Section 2 and Appendix C.

Level(s): 3

**SA-16   DEVELOPER-PROVIDED TRAINING**

Supplemental C-SCRM Guidance: Developer-provided training for external and internal (in-house) developers is critical to C-SCRM. It addresses training the individuals responsible for federal systems and networks to include applicable development environments. Developer-provided training in this control also

applies to the individuals who select system and network components. Developer-provided training should include C-SCRM material to ensure that 1) developers are aware of potential threats and vulnerabilities when developing, testing, and maintaining hardware and software; and 2) individuals responsible for selecting system and network components incorporate C-SCRM when choosing such components.

Level(s): 2, 3

Related Controls: AT-3

## SA-17 DEVELOPER SECURITY AND PRIVACY ARCHITECTURE AND DESIGN

Supplemental C-SCRM Guidance: This control facilitates the use of C-SCRM information to influence system architecture, design, and component selection decisions, including security functions. Examples include identifying components that compose system architecture and design or selecting specific components to ensure availability through multiple supplier or component selections.

Level(s): 2, 3

Related Controls: SA-17 (1) and (2)

## SA-20 CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS

Supplemental C-SCRM Guidance: The organization may decide, based on their cyber supply chain risk assessment, that they require customized development of certain critical components. This control provides additional guidance on this activity.

Level(s): 2, 3

## SA-21 DEVELOPER SCREENING

Supplemental C-SCRM Guidance: The organization should implement screening processes for their internal developers. For system integrators who may be providing key developers that address critical components, the organization should ensure that appropriate processes for developer screening have been used. Screening of developers should be included as a contractual requirement and be a flow-down requirement to relevant sub-level subcontractors who provide development services or who have access to the development environment.

Level(s): 2, 3

Control Enhancement(s):

(1) *DEVELOPER SCREENING | VALIDATION OF SCREENING*

Supplemental C-SCRM Guidance: Internal developer screening should be validated. Organizations may validate system integrator developer screening by requesting summary data from the system integrator to be provided post-validation.

Level(s): 2, 3

## SA-22 UNSUPPORTED SYSTEM COMPONENTS

Supplemental C-SCRM Guidance: Acquiring products directly from qualified original equipment manufacturers (OEMs) or their authorized distributors and resellers significantly reduces many cyber supply chain risks. In the case of unsupported system components, the organization should use authorized distributors with an ongoing relationship with the supplier of the unsupported system components.

5058
5059        When purchasing alternate sources for continued support, organizations should acquire directly from vetted
5060        original equipment manufacturers (OEMs) or their authorized distributors and resellers. Decisions about
5061        using alternate sources require input from the organization's engineering resources regarding the
5062        differences in alternate component options. For example, if an alternative is to acquire an open source
5063        software component, what are the open source community development, test, acceptance, and release
5064        processes?
5065
5066        Level(s): 2, 3
5067
5068

**FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION**

FIPS 200 specifies the System and Communications Protection minimum security requirement as follows:

> *Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.*

An organization's communications infrastructure is composed of ICT/OT components and systems, which have their own supply chains. These communications allow users or administrators to remotely access an organization's systems and to connect to the Internet, with other ICT/OT within the organization, contractor systems, and occasionally supplier systems. An organization's communications infrastructure may be provided and supported by suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

**SC-1     POLICY AND PROCEDURES**

> Supplemental C-SCRM Guidance: System and communications protection policies and procedures should address cyber supply chain risks to the organization's processes, systems, and networks. Organization-level and program-specific policies help establish and clarify these requirements and corresponding procedures provide instructions for meeting these requirements.  Policies and procedures should include the coordination of communications among and across multiple organizational entities within the organization as well as communications methods, external connections, and processes used between the organization and its suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

> Level(s): 1, 2, 3

**SC-4     INFORMATION IN SHARED RESOURCES**

> Supplemental C-SCRM Guidance: The organization may share information system resources with system suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. Protecting information in shared resources in support of various supply chain activities is challenging when outsourcing key operations. Organizations may either share too much, increasing their risk, or share too little, making it difficult for the suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers to be efficient in their service delivery. The organization should work with developers to define a structure/process of information sharing including the data shared, method of sharing, and to whom (the specific roles) it is provided. Appropriate privacy, dissemination, handling, and clearance requirements should be accounted for in the information sharing process.

> Level(s): 2, 3

**SC-5     DENIAL-OF-SERVICE PROTECTION**

Supplemental C-SCRM Guidance: C-SCRM Guidance supplemental guidance is provided in control enhancement SC-5 (2).

Control Enhancement(s):

**(2)** *DENIAL-OF-SERVICE PROTECTION | CAPACITY, BANDWIDTH, AND REDUNDANCY*

Supplemental C-SCRM Guidance: The organization should include requirements for excess capacity, bandwidth, and redundancy into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Level(s): 2

**SC-7  BOUNDARY PROTECTION**

Supplemental C-SCRM Guidance: The organization should implement appropriate monitoring mechanisms and processes at the boundaries between the agency systems and suppliers', developers', system integrators', external system service providers', and other ICT/OT-related service providers' systems. Provisions for boundary protections should be incorporated into agreements with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers. There may be multiple interfaces throughout the organization's and supplier systems and networks and the SDLC. Appropriate vulnerability, threat, and risk assessments should be performed to ensure proper boundary protections for both supply chain components as well as supply chain information flow. The vulnerability, threat, and risk assessment can aid in scoping boundary protection to a relevant set of criteria and help manage associated costs. For contracts with external service providers, organizations should ensure that the provider satisfies boundary control requirements pertinent to environments and networks within their span of control. Further detail is provided in Section 2 and Appendix C.

Level(s): 2

Control Enhancement(s):

**(13)** *BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS*

Supplemental C-SCRM Guidance: The organization should provide separation and isolation of development, test, and security assessment tools, and operational environments and relevant monitoring tools within the organization's information systems and networks. This control applies the entity responsible for creating software and hardware, to include federal agencies and prime contractors.  As such this controls applies to the federal agency and applicable supplier information systems and networks.  Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors. If a compromise or information leakage happens in any one environment, the other environments should still be protected through the separation/isolation mechanisms or techniques.

Level(s): 3

Related Controls: SR-3(3)

**(14)** *BOUNDARY PROTECTION | PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS*

Supplemental C-SCRM Guidance: This control is relevant to C-SCRM as it applies to external service providers.

Level(s): 2,3

5163          Related Controls: SR-3(3)

5164      **(19)** *BOUNDARY PROTECTION | BLOCKS COMMUNICATION FROM NON-ORGANIZATIONALLY*
5165          *CONFIGURED HOSTS*

5166          Supplemental C-SCRM Guidance: This control is relevant to C-SCRM as it applies to external service
5167          providers.
5168
5169          Level(s): 3

5170  **SC-8**  **TRANSMISSION CONFIDENTIALITY AND INTEGRITY**

5171          Supplemental C-SCRM Guidance: Requirements for transmission confidentiality and integrity should be
5172          integrated into agreements with suppliers, developers, system integrators, external system service
5173          providers, and other ICT/OT-related service providers. Acquirers, suppliers, developers, system integrators,
5174          external system service providers, and other ICT/OT-related service providers may repurpose existing
5175          security mechanisms (e.g., authentication, authorization, or encryption) to achieve organizational
5176          confidentiality and integrity requirements. The degree of protection should be based on the sensitivity of
5177          information to be transmitted and the relationship between the organization and the suppliers, developers,
5178          system integrators, external system service providers, and other ICT/OT-related service providers.
5179
5180          Level(s): 2, 3

5181  **SC-18**  **MOBILE CODE**

5182          Supplemental C-SCRM Guidance: The organization should use this control in various applications of
5183          mobile code within their information systems and networks. Examples include acquisition processes such
5184          as electronic transmission of supply chain information (e.g., email), receipt of software components,
5185          logistics information management in RFID, or transport sensors infrastructure.
5186
5187          Level(s): 3
5188
5189          Control Enhancement(s):

5190      **(2)**   *MOBILE CODE | ACQUISITION, DEVELOPMENT, AND USE*

5191          Supplemental C-SCRM Guidance: The organization should employ rigorous supply chain protection
5192          techniques in the acquisition, development, and use of mobile code to be deployed in the information
5193          system. Examples include ensuring that mobile code originates from vetted sources when acquired, that
5194          vetted system integrators are used for the development of custom mobile code or prior to installing, and
5195          that verification processes are in place for acceptance criteria prior to install in order to verify the source
5196          and integrity of code. Note that mobile code can be both code for the underlying information systems and
5197          networks (e.g., RFID device applications) or for information systems/components.
5198
5199          Level(s): 3

5200  **SC-27**  **PLATFORM-INDEPENDENT APPLICATIONS**

5201          Supplemental C-SCRM Guidance: The use of trusted platform-independent applications is essential to C-
5202          SCRM. Platform-independent applications' enhanced portability enables organizations to more readily
5203          switch external service providers in the event that one is compromised, thereby reducing vendor
5204          dependency cyber supply chain risks. This is especially relevant for critical applications that may be relied
5205          on by multiple systems.
5206
5207          Level(s): 2, 3

## SC-28    PROTECTION OF INFORMATION AT REST

Supplemental C-SCRM Guidance: The organization should include provisions for protection of
information at rest into their agreements with suppliers, developers, system integrators, external system
service providers, and other ICT/OT-related service providers. The organization should also ensure that
they provide appropriate protections within the information systems and networks for data at rest for the
suppliers, developers, system integrators, external system service providers, and other ICT/OT-related
service providers information, such as source code, testing data, blueprints, and intellectual property
information. This control should be applied throughout the SDLC including during requirements,
development, manufacturing, test, inventory management, maintenance, and disposal.  Organizations
should require its prime contractors to implement this control and flow down this requirement to relevant
sub-tier contractors.

Level(s): 2, 3

Related Controls: SR-3(3)

## SC-29    HETEROGENEITY

Supplemental C-SCRM Guidance: Heterogeneity techniques include use of different operating systems,
virtualization techniques, and multiple sources of supply. Multiple sources of supply can improve
component availability and reduce the impact of a cyber supply chain compromise. In case of a cyber
supply chain compromise, an alternative source of supply will allow the organizations to more rapidly
switch to an alternative system/component which may not be affected by the compromise. Also,
heterogeneous components decrease the attack surface by limiting the impact to the subset of the
infrastructure that is using vulnerable components.

Level(s): 2, 3

## SC-30    CONCEALMENT AND MISDIRECTION

Supplemental C-SCRM Guidance: Concealment and misdirection techniques for C-SCRM include the
establishment of random resupply times, concealment of location, random change of fake location used,
and random change/shifting of information storage into alternate servers/storage mechanisms.

Level(s): 2, 3

Control Enhancement(s):

**(2)**  *CONCEALMENT AND MISDIRECTION | RANDOMNESS*

Supplemental C-SCRM Guidance: Supply chain processes are necessarily structured with predictable,
measurable, and repeatable processes for the purpose of efficiency and cost reduction. This opens up
the opportunity for potential breach. In order to protect against compromise, the organization should
employ techniques to introduce randomness into organizational operations and assets in the
organization's systems or networks (e.g., randomly switching among several delivery organizations or
routes, or changing the time and date of receiving supplier software updates if previously predictably
scheduled).

Level(s): 2, 3

**(3)**  *CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING AND STORAGE LOCATIONS*

Supplemental C-SCRM Guidance: Changes in processing or storage locations can be used to protect
downloads, deliveries, or associated supply chain metadata. The organization may leverage such
techniques within the organizations' information systems and networks to create uncertainty into the

128

5255    activities targeted by adversaries. Establishing a few process changes and randomizing the use of them,
5256    whether it is for receiving, acceptance testing, storage, or other supply chain activities, can aid in
5257    reducing the likelihood of a supply chain event.
5258
5259    Level(s): 2, 3

5260    **(4)**  *CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION*

5261    Supplemental C-SCRM Guidance: The organization can convey misleading information as part of
5262    concealment and misdirection efforts to protect the information system being developed and the
5263    organization's systems and networks. Examples of such efforts in security include honeynets or
5264    virtualized environments. Implementations can be leveraged in conveying misleading information.
5265    These may be considered advanced techniques requiring experienced resources to effectively
5266    implement them.
5267
5268    Level(s): 2, 3

5269    **(5)**  *CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS*

5270    Supplemental C-SCRM Guidance: The organization may employ various concealment and
5271    misdirection techniques to protect information about the information system being developed and the
5272    organization's information systems and networks. For example, delivery of critical components to a
5273    central or trusted third-party depot can be used to conceal or misdirect any information regarding the
5274    component use or the organization using the component. Separating components from their associated
5275    information into differing physical and electronic delivery channels and obfuscating the information
5276    through various techniques can be used to conceal information and reduce the opportunity for potential
5277    loss of confidentiality of the component or its use, condition, and other attributes.
5278
5279    Level(s): 2, 3

5280    **SC-36    DISTRIBUTED PROCESSING AND STORAGE**

5281    Supplemental C-SCRM Guidance: Processing and storage can be distributed both across the organization's
5282    systems and networks and across the SDLC.  The organization should ensure that these techniques are
5283    applied in both contexts. The following activities can use distributed processing and storage: development,
5284    manufacturing, configuration management, test, maintenance, and operations.  This control applies to the
5285    entity responsible for processing and storage functions or related infrastructure, to include federal agencies
5286    and contractors.  As such this controls applies to the federal agency and applicable supplier information
5287    systems and networks.  Organizations should require its prime contractors to implement this control and
5288    flow down this requirement to relevant sub-tier contractors.
5289
5290    Level(s): 2, 3
5291
5292    Related Controls: SR-3(3)

5293    **SC-37    OUT-OF-BAND CHANNELS**

5294    Supplemental C-SCRM Guidance: C-SCRM-specific supplemental guidance is provided in control
5295    enhancement SC-37 (1).
5296
5297    Control Enhancement(s):

5298    **(1)**  *OUT-OF-BAND CHANNELS | ENSURE DELIVERY AND TRANSMISSION*

5299    Supplemental C-SCRM Guidance: The organization should employ security safeguards to ensure that
5300    only specific individuals or information systems receive the information about the information system

5301        or its development environment and processes. For example, proper credentialing and authorization
5302        documents should be requested and verified prior to the release of critical components such as custom
5303        chips, custom software, or information during delivery.
5304
5305        Level(s): 2, 3

5306   **SC-38**   **OPERATIONS SECURITY**

5307        Supplemental C-SCRM Guidance: The organization should ensure that appropriate supply chain threat and
5308        vulnerability information is obtained from and provided to the applicable operational security processes.
5309
5310        Level(s): 2, 3
5311
5312        Related Control(s): SR-7

5313   **SC-47**   **ALTERNATE COMMUNICATIONS PATHS**

5314        Supplemental C-SCRM Guidance: If necessary and appropriate, suppliers, developers, system integrators,
5315        external system service providers, and other ICT/OT-related service providers should be included in the
5316        alternate communication paths described in this control.
5317
5318        Level(s): 1, 2, 3

**FAMILY: SYSTEM AND INFORMATION INTEGRITY**

FIPS 200 specifies the System and Information Integrity minimum security requirement as follows:

> *Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.*

System and information integrity for systems and components traversing the supply chain is critical for managing cyber supply chain risks. Insertion of malicious code and counterfeits are two primary examples of cyber supply chain risks, both of which can at least partially be addressed by deploying system and information integrity controls. Organizations should ensure that adequate system and information integrity protections are part of C-SCRM.

**SI-1      POLICY AND PROCEDURES**

Supplemental C-SCRM Guidance: The organization should include C-SCRM in system and information integrity policy and procedures, including ensuring that program-specific requirements for employing various integrity verification tools and techniques are clearly defined. System and information integrity for information systems and components and the underlying information systems and networks is critical for managing cyber supply chain risks. Insertion of malicious code and counterfeits are two primary examples of cyber supply chain risks, both of which can be at least partially addressed by deploying system and information integrity controls.

Level(s): 1, 2, 3

Related Controls: SR-1, 9, 10, 11

**SI-2      FLAW REMEDIATION**

Supplemental C-SCRM Guidance: Output of flaw remediation activities provides useful input into ICT/OT SCRM processes described in Section 2 and Appendix C.

Level(s): 2, 3

Control Enhancement(s):

**(5)**  *FLAW REMEDIATION | AUTOMATIC SOFTWARE AND FIRMWARE UPDATES*

Supplemental C-SCRM Guidance: The organization should specify the various software assets within its information systems and networks that require automated updates (both indirect and direct). This specification of assets should be defined from criticality analysis results, which provide information on critical and noncritical functions and components (see Section 2 and Appendix C). A centralized patch management process may be employed for evaluating and managing updates prior to deployment. Those software assets that require direct updates from a supplier should only accept updates originating directly from the OEM unless specifically deployed by the acquirer, such as with a centralized patch management process.

Level(s): 2

**SI-3   MALICIOUS CODE PROTECTION**

Supplemental C-SCRM Guidance: Because the majority of code operated in federal system is not developed by the federal government, malicious code threat often originates from the supply chain. This controls applies to the federal agency and contractors with code-related responsibilities (e.g., code-development, installing patched, performing system upgrades, etc.) as well as applicable contractor information systems and networks. Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.

Level(s): 2, 3

Related Controls: SA-11; SI-7(15); SI-3(4), (6), (8), and (10); SR-3(3)

**SI-4   SYSTEM MONITORING**

Supplemental C-SCRM Guidance: This control includes monitoring of vulnerabilities resulting from past cyber supply chain compromises, such as malicious code implanted during software development and set to activate after deployment. System monitoring is frequently performed by external service providers. Service-level agreements with these providers should be structured to appropriately reflect this control.

Level(s): 1, 2, 3

Control Enhancement(s):

**(17)** *SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS*

Supplemental C-SCRM Guidance: System monitoring information may be correlated with that of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers, if appropriate. The results of correlating monitoring information may point to cyber supply chain vulnerabilities that require mitigation or compromises.

Level(s): 2, 3

**(19)** *SYSTEM MONITORING | RISK FOR INDIVIDUALS*

Supplemental C-SCRM Guidance: Persons identified as being of higher risk may include organizational employees, contractors, and other third parties (e.g., volunteers, visitors) that may have the need or ability to access to an organization's system, network, or system environment. In accordance with policies and procedures and, if relevant, terms of an agreement, and in coordination with appropriate officials, the organization may implement enhanced oversight of these higher-risk individuals.

Level(s): 2, 3

**SI-5   SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**

Supplemental C-SCRM Guidance: The organization should evaluate security alerts, advisories, and directives for cyber supply chain impact and follow up if needed. U.S. Cert, FASC, and other authoritative entities, generate security alerts and advisories that are applicable to C-SCRM. Additional laws and regulations will impact who and how additional advisories are provided. Organizations should ensure their information sharing protocols and processes include sharing alerts, advisories, and directives with relevant parties with whom they have an agreement to deliver products or perform services. Organization's should provide direction or guidance as to what actions are to be taken in response to sharing such an alert, advisory, or directive.

5411
5412        <u>Level(s)</u>: 1, 2, 3

5413   **SI-7**   **SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY**

5414        <u>Supplemental C-SCRM Guidance</u>: This control applies to the federal agency and applicable supplier
5415        information systems and networks. The integrity of all applicable systems and networks should be
5416        systematically tested and verified to ensure that it remains as required so that the systems/components
5417        traversing through the supply chain are not impacted by unanticipated changes. The integrity of systems
5418        and components should also be tested and verified. Applicable verification tools include: digital signature
5419        or checksum verification, acceptance testing for physical components, confining software to limited
5420        privilege environments such as sandboxes, code execution in contained environments prior to use, and
5421        ensuring that if only binary or machine-executable code is available, it is obtained directly from the OEM
5422        or a verified supplier or distributer. Mechanisms for this control are discussed in detail in NIST SP 800-53
5423        Rev. 5. This controls applies to the federal agency and applicable supplier information systems and
5424        networks.  When purchasing an ICT/OT product, an organization should perform due diligence to
5425        understand what a supplier's integrity assurance practices are. Organizations should require its prime
5426        contractors to implement this control and flow down this requirement to relevant sub-tier contractors.
5427
5428        <u>Level(s)</u>: 2, 3
5429
5430        <u>Related Controls</u>: SR-3(3)
5431
5432        <u>Control Enhancement(s)</u>:

5433        **(14)** *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | BINARY OR MACHINE EXECUTABLE*
5434            *CODE*

5435            <u>Supplemental C-SCRM Guidance</u>: The organization should obtain binary or machine-executable code
5436            directly from the OEM/developer or other verified source.
5437
5438            <u>Level(s)</u>: 2, 3

5439        **(15)** *SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION*

5440            <u>Supplemental C-SCRM Guidance</u>: The organization should ensure that code authentication
5441            mechanisms such as digital signatures are implemented to assure the integrity of software, firmware,
5442            and information.

5443            <u>Level(s)</u>: 3

5444   **SI-12**   **INFORMATION MANAGEMENT AND RETENTION**

5445        <u>Supplemental C-SCRM Guidance</u>: C-SCRM should be included in information management and retention
5446        requirements, especially when system integrator, supplier, and external service provider sensitive and
5447        proprietary information is concerned.
5448
5449        <u>Level(s)</u>: 3

5450   **SI-20**   **TAINTING**

5451        <u>Supplemental C-SCRM Guidance</u>: Suppliers, developers, system integrators, external system service
5452        providers, and other ICT/OT-related service providers may have access to federal agency sensitive
5453        information.  If that is the case, organizations should require its prime contractors to implement this control
5454        and flow down this requirement to relevant sub-tier contractors.
5455

5456          Level(s): 2, 3
5457
5458          Related Controls: SR-9

**FAMILY: SUPPLY CHAIN RISK MANAGEMENT**

FIPS 200 does not specify Supply Chain Risk Management minimum security requirements. NIST SP 800-53 Rev. 5 established a new control family: Supply Chain Risk Management. Supplemental guidance below expands upon the SR controls and provides further information and context for their application.

**SR-1    POLICY AND PROCEDURES**

Supplemental C-SCRM Guidance: C-SCRM policies is developed at Level 1 for the overall organization and at Level 2 for specific missions and functions. C-SCRM policies can be implemented at Levels 1, 2, and 3, depending on the level of depth and detail. C-SCRM procedures are developed at Level 2 for specific missions and functions and at Level 3 for specific systems. Organizational functions including but not limited to information security, legal, risk management, and acquisition should review and concur on the development of C-SCRM policies and procedures or providing guidance to system owners for developing system-specific C-SCRM procedures.

Level(s): 1, 2, 3

**SR-2    SUPPLY CHAIN RISK MANAGEMENT PLAN**

Supplemental C-SCRM Guidance: C-SCRM plans describes implementations, requirements, constraints, and implications at the system level. C-SCRM plans are influenced by the organization's other risk assessment activities and may inherit and tailor common control baselines defined at Level 1 and 2. C-SCRM plans defined at Level 3 works in collaboration with the organization's C-SCRM Strategy and Policies (Levels 1 & 2), and the C-SCRM Implementation Plan (Levels 1 & 2) to provide a systematic and holistic approach for cyber supply chain risk management across the organization.

C-SCRM plans should be developed as a standalone document and only integrated in existing system security plans if organizational constraints require it.

Level(s): 3

Related Controls: PL-2

**SR-3    SUPPLY CHAIN CONTROLS AND PROCESSES**

Supplemental C-SCRM Guidance: Section 2 and Appendix C of this document provide detailed guidance on implementing this control.

Level(s): 1, 2, 3

Control Enhancement(s):

**(1)** *SUPPLY CHAIN CONTROLS AND PROCESSES | DIVERSE SUPPLY BASE*

Supplemental C-SCRM Guidance: Organizations should diversify their supply base, especially for critical ICT/OT products and services. As a part of this exercise the organization should attempt to identify single points of failure and risk among primes and lower level entities in the supply chain. Criticality analysis as described in NISTIR 8272, *Impact Analysis Tool for Interdependent Cyber*

*Supply Chain Risks* can help determine which suppliers are critical. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.

Level(s): 2, 3

Related Controls: RA-9

**(3)** *SUPPLY CHAIN CONTROLS AND PROCESSES | SUB-TIER FLOW DOWN*

Supplemental C-SCRM Guidance:  Organizations should require its prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors throughout the SDLC. The use of the acquisition process provides an important vehicle to protect the supply chain. Organization should include as part of procurement requirements the need for suppliers to flow down controls to subcontractors throughout the SDLC.  As part of market research and analysis activities, organization should conduct robust due diligence research on potential suppliers or products as well as their upstream dependencies (i.e., 4th and 5th party suppliers). The results of this research can be helpful in shaping the sourcing approach and refining requirements. Then, during the solicitation and contract award phase, an evaluation of the cyber supply chain risks associated with a supplier, product, or service should be completed prior to the contract award decision to ensure the holistic risk profile is well understood and serves as a weighted factor in award decisions. During the period of performance, suppliers should be monitored for conformance to the defined controls and requirements, as well as changes in risk conditions. See Section 3 for guidance on the Role of C-SCRM in the Acquisition Process.

Level(s): 2, 3

**SR-4    PROVENANCE**

Supplemental C-SCRM Guidance:  Provenance should be applied to systems, system components, and associated data throughout the SDLC.

Level(s): 2, 3

**SR-5    ACQUISITION STRATEGIES, TOOLS, AND METHODS**

Supplemental C-SCRM Guidance:  Section 3 and SA controls provide additional guidance on acquisition strategies, tools, and methods.

Level(s): 1, 2, 3

Related Controls: SA Control Family

**SR-6    SUPPLIER ASSESSMENTS AND REVIEWS**

Supplemental C-SCRM Guidance:  In general, an organization should consider any information pertinent to the security, integrity, resilience, quality, trustworthiness, or authenticity of the supplier, or their provided services or products. Organizations should consider applying this information against a consistent set of core, baseline factors and assessment criteria to facilitate equitable comparison (between suppliers as well as over time). Depending upon the specific context and purpose for which the assessment is being conducting, the organization may select additional factors. The quality of information (e.g., its relevance,

5545  completeness, accuracy, etc.) relied upon for an assessment is also an important consideration.  Reference
5546  sources for assessment information should also be documented. The C-SCRM PMO can help define
5547  requirements, methods, and tools for organization's supplier assessments.

5548
5549  Level(s): 2, 3
5550

5551  **SR-7    SUPPLY CHAIN OPERATIONS SECURITY**

5552  Supplemental C-SCRM Guidance: C-SCRM PMO can help determine OPSEC controls that apply to
5553  specific missions and functions.  OPSEC controls are particularly important when there is specific concern
5554  about an adversarial threat from or to the organization's supply chain or an element within the supply chain
5555  or the nature of the organization's mission or business operations, its information, and/or its service/product
5556  offerings may make it a more attractive target of an adversarial threat.

5557
5558  Level(s): 2, 3
5559

5560  **SR-8    NOTIFICATION AGREEMENTS**

5561  Supplemental C-SCRM Guidance: Organizations should require their suppliers, minimally, have
5562  established notification agreements with those entities within their supply chain that have a role or
5563  responsibility related to that critical service or product.

5564  Level(s): 2, 3
5565
5566  Related Controls: RA-9

5567

5568  **SR-9    TAMPER RESISTANCE AND DETECTION**

5569  Supplemental C-SCRM Guidance: Organizations should apply tamper resistance and detection control to
5570  critical components, at a minimum.  Criticality analysis can help determine which components are critical.
5571  See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.  C-SCRM PMO can
5572  help identify critical components, especially those that are used by multiple missions, functions, and
5573  systems within an organization.

5574  Level(s): 2, 3
5575
5576  Related Controls: RA-9

5577

5578  **SR-10   INSPECTION OF SYSTEMS OR COMPONENTS**

5579  Supplemental C-SCRM Guidance:  Organizations should inspect critical systems and components, at a
5580  minimum, for assurance that tamper resistance controls are in place and to examine whether there is
5581  evidence of tampering. Products or components should be inspected prior to use and periodically thereafter.
5582  Inspection requirements should also be included in contracts with suppliers, developers, system integrators,
5583  external system service providers, and other ICT/OT-related service providers. Organizations should
5584  require its prime contractors to implement this control and flow down this requirement to relevant sub-tier
5585  contractors and flow down to subcontractors, when relevant.

5586 Criticality analysis can help determine which systems and components are critical and should therefore be
5587 subjected to inspection. See Section 2, Appendix C, and RA-9 for guidance on conducting criticality
5588 analysis.  C-SCRM PMO can help identify critical systems and components, especially those that are used
5589 by multiple missions, functions, and systems (for components) within an organization.

5590 Level(s): 2, 3
5591
5592 Related Controls: RA-9

5593

5594 **SR-11 COMPONENT AUTHENTICITY**

5595 Supplemental C-SCRM Guidance:  Development of anti-counterfeit policy and procedures requires input
5596 from and coordination with acquisition, Information Technology, IT Security, legal, and the C-SCRM
5597 PMO.  The policy and procedures should address regulatory compliance requirements, contract
5598 requirements/clauses as well as counterfeit reporting processes to organizations such as GIDEP and/or
5599 other appropriate organizations.

5600 Level(s): 1, 2, 3
5601

5602 Control Enhancement(s):

5603 **(1)** *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING*
5604 Supplemental C-SCRM Guidance:  C-SCRM PMO can assist in identifying resources that can provide
5605 anti-counterfeit training and/or may be able to conduct such training for the organization.  The C-
5606 SCRM PMO can also assist in identifying which personnel should receive the training.
5607
5608 Level(s): 2, 3

5609
5610 **(2)** *COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR*
5611 Supplemental C-SCRM Guidance:  Information Technology, IT Security, or the C-SCRM PMO should
5612 be responsible for establishing and implementing configuration control processes for component
5613 service and repair, to include, if applicable, integrating component service and repair into the overall
5614 organizational configuration control processes.  Component authenticity should be addressed in
5615 contracts when procuring component servicing and repair support.
5616
5617 Level(s): 2, 3
5618

5619 **(3)** *COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING*
5620 Supplemental C-SCRM Guidance:  Organizations should conduct anti-counterfeit scanning for critical
5621 components, at a minimum.  Criticality analysis can help determine which components are critical and
5622 should be subjected to this scanning. See Section 2, Appendix C, and RA-9 for guidance on conducting
5623 criticality analysis.  C-SCRM PMO can help identify critical components, especially those that are
5624 used by multiple missions, functions, and systems within an organization.
5625
5626 Level(s): 2, 3

5627 Related Controls: RA-9

5628

5629 **SR-12 COMPONENT DISPOSAL**

5630
5631

Supplemental C-SCRM Guidance:  IT Security, in coordination with the C-SCRM PMO, can help establish appropriate component disposal policies, procedures, mechanisms, and techniques.

5632

Level(s): 2, 3

5633

5634 **SR-13   SUPPLIER INVENTORY (NEW)**

5635

Control:

5636
5637

a.   Develop, document, and maintain an accurate and complete inventory of suppliers that present cyber supply chain risk. This inventory should:

5638

  1.   Document organization's suppliers;

5639

  2.   Identify whether the supplier provides a product and/or service;

5640
5641

  3.   For each supplier, indicate which programs, projects, and systems are using supplier products and services

5642
5643

  4.   For each supplier, assign criticality level to each supplier organization that aligns to the criticality of the program, project and/or system (or component of system).

5644

b.   Review and update supplier inventory [*Assignment: organization-defined frequency*].

5645
5646
5647
5648
5649
5650
5651
5652

Supplemental C-SCRM Guidance:  Organizations rely on numerous suppliers to execute their missions and functions.  Many suppliers provide products and services in support of multiple missions, functions, programs, projects, and systems.  Some suppliers are more critical than others, based on the criticality of missions, functions, programs, projects, systems that their products and services support, as well as the organization's level of dependency on the supplier.  Organizations should use criticality analysis to help determine which products and services are critical to determine criticality of suppliers to be documented in the supplier inventory.  See Section 2, Appendix C, and RA-9 for guidance on conducting criticality analysis.

5653

Level(s): 2, 3

5654
5655

Related Controls: RA-9

5656
5657
5658

5659
5660 **APPENDIX A: C-SCRM CONTROL SUMMARY**

5661 This appendix lists the C-SCRM controls in this publication and maps them to their
5662 corresponding NIST SP 800-53 Rev. 5 controls as appropriate. Table A-1 indicates those
5663 controls that are defined in NIST SP 800-53 Rev. 5 Low baseline requirements and are deemed
5664 to be C-SCRM relevant. Some C-SCRM controls were added to this baseline to form the C-
5665 SCRM Baseline. Additionally, controls that should flow down from prime contractors to their
5666 relevant sub-tier contractors are listed as Flow Down Controls. Given that C-SCRM is an
5667 organization-wide activity that requires selection and implementation of controls at the
5668 enterprise, mission/business, and operational levels (Levels 1, 2, and 3 of the organization
5669 according to NIST SP 800-39), Table A-1 indicates the organizational levels in which the
5670 controls should be implemented. The table highlights C-SCRM controls and enhancements not in
5671 NIST SP 800-53 Rev. 5 in red, viz., MA-8 and SR-13.
5672
5673 **Table A-1: C-SCRM Control Summary**

| Control Identifier | Control (or Control Enhancement) Name | C-SCRM Baseline | Flow Down Control | Levels | | |
|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 |
| AC-1 | **Policy and Procedures** | x | x | x | x | x |
| AC-2 | **Account Management** | x | | | x | x |
| AC-3 | **Access Enforcement** | x | | | x | x |
| AC-3(8) | *Access Enforcement | Revocation of Access Authorizations* | | | | x | x |
| AC-3(9) | *Access Enforcement | Controlled Release* | | | | x | x |
| AC-4 | **Information Flow Enforcement** | | x | | x | x |
| AC-4(6) | *Information Flow Enforcement | Metadata* | | | | x | x |
| AC-4(17) | *Information Flow Enforcement | Domain Authentication* | | | | x | x |
| AC-4(19) | *Information Flow Enforcement | Validation of Metadata* | | | | x | x |
| AC-4(21) | *Information Flow Enforcement | Physical or Logical Separation of Information Flows* | | | | | x |
| AC-5 | **Separation of Duties** | | | | x | x |
| (AC-6) | **(Least Privilege)** | (x) | (N/A) | | | |
| AC-6(6) | *Least Privilege | Privileged Access by Non-organizational Users* | | | | x | x |
| AC-17 | **Remote Access** | x | x | | x | x |
| AC-17(6) | *Remote Access | Protection of Mechanism Information* | | | | x | x |
| AC-18 | **Wireless Access** | x | | x | x | x |
| AC-19 | **Access Control for Mobile Devices** | x | | | x | x |
| AC-20 | **Use of External Systems** | x | x | x | x | x |
| AC-20(1) | *Use of External Systems | Limits on Authorized Use* | | | | x | x |
| AC-20(3) | *Use of External Systems | Non-organizationally Owned Systems — Restricted Use* | | | | x | x |
| AC-21 | **Information Sharing** | | | x | x | |
| AC-22 | **Publicly Accessible Content** | x | | | x | x |
| AC-23 | **Data Mining Protection** | | x | | x | x |
| AC-24 | **Access Control Decisions** | | x | x | x | x |
| AT-1 | **Policy and Procedures** | x | | x | x | |
| (AT-2) | **(Literacy Training and Awareness)** | (x) | (N/A) | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| AT-2(1) | *Literacy Training and Awareness | Practical Exercises* | | | | x | |
| AT-2(2) | *Literacy Training and Awareness | Insider Threat* | x | x | | x | |
| AT-2(3) | *Literacy Training and Awareness | Social Engineering and Mining* | | | | x | |
| AT-2(4) | *Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior* | | | | x | |
| AT-2(5) | *Literacy Training and Awareness | Advanced Persistent Threat* | | | | x | |
| AT-2(6) | *Literacy Training and Awareness | Cyber Threat Environment* | | | | x | |
| **AT-3** | **Role-based Training** | x | | | x | |
| AT-3(2) | *Role-based Training | Physical Security Controls* | | | | x | |
| **AT-4** | **Training Records** | x | | | x | |
| **AU-1** | **Policy and Procedures** | x | | x | x | x |
| **AU-2** | **Event Logging** | x | | x | x | x |
| **AU-3** | **Content of Audit Records** | x | | x | x | x |
| **AU-6** | **Audit Record Review, Analysis, and Reporting** | x | | | x | x |
| AU-6(9) | *Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources* | | | | | x |
| **AU-10** | **Non-repudiation** | | | | | x |
| AU-10(1) | *Non-repudiation | Association of Identities* | | | | x | |
| AU-10(2) | *Non-repudiation | Validate Binding of Information Producer Identity* | | | | x | x |
| AU-10(3) | *Non-repudiation | Chain of Custody* | | | | x | x |
| **AU-12** | **Audit Record Generation** | x | | | x | x |
| **AU-13** | **Monitoring for Information Disclosure** | | | | x | x |
| **AU-14** | **Session Audit** | | | | x | x |
| **AU-16** | **Cross-organizational Audit Logging** | | | | x | x |
| AU-16(2) | *Cross-organizational Audit Logging | Sharing of Audit Information* | | x | | x | x |
| **CA-1** | **Policy and Procedures** | x | | x | x | x |
| **CA-2** | **Control Assessments** | x | | | x | x |
| CA-2(2) | *Control Assessments | Specialized Assessments* | | | | | x |
| CA-2(3) | *Control Assessments | Leveraging Results from External Organizations* | | | | | x |
| **CA-3** | **Information Exchange** | x | x | | | x |
| **CA-5** | **Plan of Action and Milestones** | x | | | x | x |
| **CA-6** | **Authorization** | x | | x | x | x |
| **(CA-7)** | **(Continuous Monitoring)** | (x) | (N/A) | | | |
| CA-7(3) | *Continuous Monitoring | Trend Analyses* | | | | | x |
| **CM-1** | **Policy and Procedures** | x | | x | x | x |
| **CM-2** | **Baseline Configuration** | x | | | x | x |
| CM-2(6) | *Baseline Configuration | Development and Test Environments* | | | | x | x |
| **CM-3** | **Configuration Change Control** | | | | x | x |
| CM-3(1) | *Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes* | | | | x | x |
| CM-3(2) | *Configuration Change Control | Testing, Validation, and Documentation of Changes* | | | | x | x |
| CM-3(4) | *Configuration Change Control | Security and Privacy Representatives* | | | | x | x |

| | | | | | | |
|---|---|---|---|---|---|---|
| CM-3(8) | *Configuration Change Control | Prevent or Restrict Configuration Changes* | | | | x | x |
| **CM-4** | **Impact Analyses** | x | | | | x |
| CM-4(1) | *Impact Analyses | Separate Test Environments* | | | | | x |
| **CM-5** | **Access Restrictions for Change** | x | | | x | x |
| CM-5(1) | *Access Restrictions for Change | Automated Access Enforcement and Audit Records* | | | | | x |
| CM-5(6) | *Access Restrictions for Change | Limit Library Privileges* | | | | | x |
| **CM-6** | **Configuration Settings** | x | | | x | x |
| CM-6(1) | *Configuration Settings | Automated Management, Application, and Verification* | | | | | x |
| CM-6(2) | *Configuration Settings | Respond to Unauthorized Changes* | | | | | x |
| **CM-7** | **Least Functionality** | x | x | | | x |
| CM-7(1) | *Least Functionality | Periodic Review* | | | | x | x |
| CM-7(4) | *Least Functionality | Unauthorized Software* | | | | x | x |
| CM-7(5) | *Least Functionality | Authorized Software* | | | | | x |
| CM-7(6) | *Least Functionality | Confined Environments with Limited Privileges* | | | | x | x |
| CM-7(7) | *Least Functionality | Code Execution in Protected Environments* | | | | | x |
| CM-7(8) | *Least Functionality | Binary or Machine Executable Code* | | | | x | x |
| CM-7(9) | *Least Functionality | Prohibiting the Use of Unauthorized Hardware* | | | | x | x |
| **CM-8** | **System Component Inventory** | x | | | x | x |
| CM-8(1) | *System Component Inventory | Updates During Installation and Removal* | | | | | x |
| CM-8(2) | *System Component Inventory | Automated Maintenance* | | | | | x |
| CM-8(4) | *System Component Inventory | Accountability Information* | | | | | x |
| CM-8(6) | *System Component Inventory | Assessed Configurations and Approved Deviations* | | | | | x |
| CM-8(7) | *System Component Inventory | Centralized Repository* | | | | | x |
| CM-8(8) | *System Component Inventory | Automated Location Tracking* | | | | x | x |
| CM-8(9) | *System Component Inventory | Assignment of Components to Systems* | | | | | x |
| **CM-9** | **Configuration Management Plan** | | x | | x | x |
| CM-9(1) | *Configuration Management Plan | Assignment of Responsibility* | | | | x | x |
| **CM-10** | **Software Usage Restrictions** | x | | | x | x |
| CM-10(1) | *Software Usage Restrictions | Open-source Software* | | | | x | x |
| **CM-11** | **User-installed Software** | x | | | x | x |
| **CM-12** | **Information Location** | | | | x | x |
| CM-12(1) | *Information Location | Automated Tools to Support Information Location* | | | | x | x |
| **CM-13** | **Data Action Mapping** | | | | x | x |
| **CM-14** | **Signed Components** | | | | | x |
| **CP-1** | **Policy and Procedures** | x | | x | x | x |
| **CP-2** | **Contingency Plan** | x | | | x | x |
| CP-2(1) | *Contingency Plan | Coordinate with Related Plans* | | | | x | x |

| | | | | | | |
|---|---|---|---|---|---|---|
| CP-2(2) | *Contingency Plan \| Capacity Planning* | | | | x | x |
| CP-2(7) | *Contingency Plan \| Coordinate with External Service Providers* | | x | | | x |
| CP-2(8) | *Contingency Plan \| Identify Critical Assets* | | | | | x |
| **CP-3** | **Contingency Training** | x | | | x | x |
| CP-3(1) | *Contingency Training \| Simulated Events* | | | | x | x |
| **CP-4** | **Contingency Plan Testing** | x | | | x | x |
| **CP-6** | **Alternate Storage Site** | | | | x | x |
| CP-6(1) | *Alternate Storage Site \| Separation from Primary Site* | | | | x | x |
| **CP-7** | **Alternate Processing Site** | | | | x | x |
| **CP-8** | **Telecommunications Services** | | | | x | x |
| CP-8(3) | *Telecommunications Services \| Separation of Primary and Alternate Providers* | | | | x | x |
| CP-8(4) | *Telecommunications Services \| Provider Contingency Plan* | | | | x | x |
| **CP-11** | **Alternate Communications Protocols** | | | | x | x |
| **IA-1** | **Policy and Procedures** | x | | x | x | x |
| **IA-2** | **Identification and Authentication (organizational Users)** | x | | x | x | x |
| **IA-3** | **Device Identification and Authentication** | | | x | x | x |
| **IA-4** | **Identifier Management** | x | | | x | x |
| IA-4(6) | *Identifier Management \| Cross-organization Management* | | | x | x | x |
| **IA-5** | **Authenticator Management** | x | | | x | x |
| IA-5(5) | *Authenticator Management \| Change Authenticators Prior to Delivery* | | | | | x |
| IA-5(9) | *Authenticator Management \| Federated Credential Management* | | | | | x |
| **IA-8** | **Identification and Authentication (non-organizational Users)** | x | | | x | x |
| **IA-9** | **Service Identification and Authentication** | | | | x | x |
| **IR-1** | **Policy and Procedures** | x | x | x | x | x |
| **IR-2** | **Incident Response Training** | x | | | x | x |
| **(IR-4)** | **(Incident Handling)** | (x) | (N/A) | | | |
| **IR-3** | **Incident Response Testing** | | | | x | x |
| IR-4(6) | *Incident Handling \| Insider Threats* | | | x | x | x |
| IR-4(7) | *Incident Handling \| Insider Threats — Intra-organization Coordination* | | | x | x | x |
| IR-4(10) | *Incident Handling \| Supply Chain Coordination* | | x | | x | |
| IR-4(11) | *Incident Handling \| Integrated Incident Response Team* | | | | | x |
| **IR-5** | **Incident Monitoring** | x | | | x | x |
| **(IR-6)** | **(Incident Reporting)** | (x) | (N/A) | | | |
| IR-6(3) | *Incident Reporting \| Supply Chain Coordination* | | x | | | x |
| **(IR-7)** | **(Incident Response Assistance)** | (x) | (N/A) | | | |
| IR-7(2) | *Incident Response Assistance \| Coordination with External Providers* | | x | | | x |
| **IR-8** | **Incident Response Plan** | x | x | | x | x |
| **IR-9** | **Information Spillage Response** | | x | | | x |
| **MA-1** | **Policy and Procedures** | x | x | x | x | x |
| **(MA-2)** | **(Controlled Maintenance)** | (x) | (N/A) | | | |
| MA-2(2) | *Controlled Maintenance \| Automated Maintenance Activities* | | | | | x |

143

| ID | Control Name | | | | | |
|---|---|---|---|---|---|---|
| **MA-3** | **Maintenance Tools** | | | | x | x |
| MA-3(1) | *Maintenance Tools \| Inspect Tools* | | | | | x |
| MA-3(2) | *Maintenance Tools \| Inspect Media* | | | | | x |
| MA-3(3) | *Maintenance Tools \| Prevent Unauthorized Removal* | | | | | x |
| **MA-4** | **Nonlocal Maintenance** | x | x | | x | x |
| MA-4(3) | *Nonlocal Maintenance \| Comparable Security and Sanitization* | | | | x | x |
| **MA-5** | **Maintenance Personnel** | x | | | x | x |
| MA-5(4) | *Maintenance Personnel \| Foreign Nationals* | | x | | x | x |
| **MA-6** | **Timely Maintenance** | | | | | x |
| **MA-7** | **Field Maintenance** | | | | | x |
| **MA-8** | **Maintenance Monitoring and Information Sharing** | | | | | x |
| **MP-1** | **Policy and Procedures** | x | | x | x | |
| **MP-4** | **Media Storage** | | x | x | x | |
| **MP-5** | **Media Transport** | | | x | x | |
| **MP-6** | **Media Sanitization** | x | x | | x | x |
| **PE-1** | **Policy and Procedures** | x | | x | x | x |
| **PE-2** | **Physical Access Authorizations** | x | x | | x | x |
| PE-2(1) | *Physical Access Authorizations \| Access by Position or Role* | | | | x | x |
| **PE-3** | **Physical Access Control** | x | | | x | x |
| PE-3(1) | *Physical Access Control \| System Access* | | | | x | x |
| PE-3(2) | *Physical Access Control \| Facility and Systems* | | | | x | x |
| PE-3(5) | *Physical Access Control \| Tamper Protection* | | | | x | x |
| **PE-6** | **Monitoring Physical Access** | x | | x | x | x |
| **PE-16** | **Delivery and Removal** | x | | | | x |
| **PE-17** | **Alternate Work Site** | | | | | x |
| **PE-18** | **Location of System Components** | | | x | x | x |
| **PE-20** | **Asset Monitoring and Tracking** | | | | x | x |
| **PE-23** | **Facility Location** | | x | | x | x |
| **PL-1** | **Policy and Procedures** | x | | | x | |
| **PL-2** | **System Security and Privacy Plans** | x | x | | | x |
| **PL-4** | **Rules of Behavior** | x | | | x | x |
| **PL-7** | **Concept of Operations** | | | | | x |
| **PL-8** | **Security and Privacy Architectures** | | | | x | x |
| PL-8(2) | *Security and Privacy Architectures \| Supplier Diversity* | | | | x | x |
| **PL-9** | **Central Management** | | | x | x | |
| **PL-10** | **Baseline Selection** | x | | | x | x |
| **PM-2** | **Information Security Program Leadership Role** | | | x | x | |
| **PM-3** | **Information Security and Privacy Resources** | | | x | x | |
| **PM-4** | **Plan of Action and Milestones Process** | | | | x | x |
| **PM-5** | **System Inventory** | | | | x | x |
| **PM-6** | **Measures of Performance** | | | x | x | |
| **PM-7** | **Enterprise Architecture** | | | x | x | |
| **PM-8** | **Critical Infrastructure Plan** | | | x | | |
| **PM-9** | **Risk Management Strategy** | | | x | | |
| **PM-10** | **Authorization Process** | | | x | x | |
| **PM-11** | **Mission and Business Process Definition** | | | x | x | x |
| **PM-12** | **Insider Threat Program** | | | x | x | x |
| **PM-13** | **Security and Privacy Workforce** | | | x | x | |
| **PM-14** | **Testing, Training, and Monitoring** | | | x | x | |
| **PM-15** | **Security and Privacy Groups and Associations** | | | x | x | |

| | | | | | | |
|---|---|---|---|---|---|---|
| PM-16 | **Threat Awareness Program** | | | x | x | |
| PM-17 | **Protecting Controlled Unclassified Information on External Systems** | | | | x | |
| PM-18 | **Privacy Program Plan** | | x | x | x | |
| PM-19 | **Privacy Program Leadership Role** | | | x | | |
| PM-20 | **Dissemination of Privacy Program Information** | | | x | x | |
| PM-21 | **Accounting of Disclosures** | | | x | x | |
| PM-22 | **Personally Identifiable Information Quality Management** | | | x | x | |
| PM-23 | **Data Governance Body** | | | x | | |
| PM-25 | **Minimization of Personally Identifiable Information Used in Testing, Training, and Research** | | | | x | |
| PM-26 | **Complaint Management** | | | | x | x |
| PM-27 | **Privacy Reporting** | | | | x | x |
| PM-28 | **Risk Framing** | | | x | | |
| PM-29 | **Risk Management Program Leadership Roles** | | | x | | |
| PM-30 | **Supply Chain Risk Management Strategy** | | | x | x | |
| PM-31 | **Continuous Monitoring Strategy** | | | x | x | x |
| PM-32 | **Purposing** | | | | x | x |
| PS-1 | **Policy and Procedures** | x | x | x | x | x |
| PS-3 | **Personnel Screening** | x | x | | x | x |
| PS-6 | **Access Agreements** | x | x | | x | x |
| PS-7 | **External Personnel Security** | x | | | x | |
| PT-1 | **Policy and Procedures** | | x | x | x | x |
| RA-1 | **Policy and Procedures** | x | | x | x | x |
| RA-2 | **Security Categorization** | x | | x | x | x |
| RA-3 | **Risk Assessment** | x | | x | x | x |
| RA-5 | **Vulnerability Monitoring and Scanning** | x | | | x | x |
| RA-5(3) | *Vulnerability Monitoring and Scanning | Breadth and Depth of Coverage* | | | | x | x |
| RA-5(6) | *Vulnerability Monitoring and Scanning | Automated Trend Analyses* | | | | x | x |
| RA-7 | **Risk Response** | x | | x | x | x |
| RA-9 | **Criticality Analysis** | | | x | x | x |
| RA-10 | **Threat Hunting** | | | x | x | x |
| SA-1 | **Policy and Procedures** | x | | x | x | x |
| SA-2 | **Allocation of Resources** | x | | x | x | |
| SA-3 | **System Development Life Cycle** | x | | x | x | x |
| SA-4 | **Acquisition Process** | x | | x | x | x |
| SA-4(5) | *Acquisition Process | System, Component, and Service Configurations* | | | | | x |
| SA-4(7) | *Acquisition Process | NIAP-approved Protection Profiles* | | | | x | x |
| SA-4(8) | *Acquisition Process | Continuous Monitoring Plan for Controls* | | | | x | x |
| SA-5 | **System Documentation** | x | | | | x |
| SA-8 | **Security and Privacy Engineering Principles** | x | | x | x | x |
| **(SA-9)** | **(External System Services)** | (x) | (N/A) | | | |
| SA-9(1) | *External System Services | Risk Assessments and Organizational Approvals* | | | | x | x |
| SA-9(3) | *External System Services | Establish and Maintain Trust Relationship with Providers* | | | x | x | x |

| SA-9(4) | *External System Services | Consistent Interests of Consumers and Providers* | | | | | x |
|---|---|---|---|---|---|---|---|
| SA-9(5) | *External System Services | Processing, Storage, and Service Location* | | | | | | x |
| **SA-10** | **Developer Configuration Management** | | | | | x | x |
| **SA-11** | **Developer Testing and Evaluation** | | | | x | x | x |
| **SA-15** | **Development Process, Standards, and Tools** | | | | | x | x |
| SA-15(3) | *Development Process, Standards, and Tools | Criticality Analysis* | | | | | x | x |
| SA-15(4) | *Development Process, Standards, and Tools | Threat Modeling and Vulnerability Analysis* | | | | | x | x |
| SA-15(8) | *Development Process, Standards, and Tools | Reuse of Threat and Vulnerability Information* | | | | | | x |
| **SA-16** | **Developer-provided Training** | | | | | x | x |
| **SA-17** | **Developer Security and Privacy Architecture and Design** | | | | | x | x |
| **SA-20** | **Customized Development of Critical Components** | | | | | x | x |
| **SA-21** | **Developer Screening** | | | x | | x | x |
| SA-21(1) | *Developer Screening | Validation of Screening* | | | | | x | x |
| **SA-22** | **Unsupported System Components** | x | | | | x | x |
| **SC-1** | **Policy and Procedures** | x | | | x | x | x |
| **SC-4** | **Information in Shared System Resources** | | | | | x | x |
| **(SC-5)** | **(Denial-of-service Protection)** | (x) | (N/A) | | | | |
| SC-5(2) | *Denial-of-service Protection | Capacity, Bandwidth, and Redundancy* | | | | | x | |
| **SC-7** | **Boundary Protection** | x | | | | x | |
| SC-7(13) | *Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components* | | x | | | | x |
| SC-7(14) | *Boundary Protection | Protect Against Unauthorized Physical Connections* | | | | | x | x |
| SC-7(19) | *Boundary Protection | Block Communication from Non-organizationally Configured Hosts* | | | | | | x |
| **SC-8** | **Transmission Confidentiality and Integrity** | | | | | x | x |
| **SC-18** | **Mobile Code** | | | | | | x |
| SC-18(2) | *Mobile Code | Acquisition, Development, and Use* | | | | | | x |
| **SC-27** | **Platform-independent Applications** | | | | | x | x |
| **SC-28** | **Protection of Information at Rest** | | x | | | x | x |
| **SC-29** | **Heterogeneity** | | | | | x | x |
| **SC-30** | **Concealment and Misdirection** | | | | | x | x |
| SC-30(2) | *Concealment and Misdirection | Randomness* | | | | | x | x |
| SC-30(3) | *Concealment and Misdirection | Change Processing and Storage Locations* | | | | | x | x |
| SC-30(4) | *Concealment and Misdirection | Misleading Information* | | | | | x | x |
| SC-30(5) | *Concealment and Misdirection | Concealment of System Components* | | | | | x | x |
| **SC-36** | **Distributed Processing and Storage** | | x | | | x | x |
| **(SC-37)** | **(Out-of-band Channels)** | (x) | (N/A) | | | | x |
| SC-37(1) | *Out-of-band Channels | Ensure Delivery and Transmission* | | | | | x | x |
| **SC-38** | **Operations Security** | | | | | x | x |
| **SC-47** | **Alternate Communications Paths** | | | | x | x | x |

| | | | | | | |
|---|---|---|---|---|---|---|
| SI-1 | **Policy and Procedures** | x | | | x | x | x |
| SI-2 | **Flaw Remediation** | x | | | x | x |
| SI-2(5) | *Flaw Remediation | Automatic Software and Firmware Updates* | | | | x | |
| SI-3 | **Malicious Code Protection** | x | x | | x | x |
| SI-4 | **System Monitoring** | x | | x | x | x |
| SI-4(17) | *System Monitoring | Integrated Situational Awareness* | | | | x | x |
| SI-4(19) | *System Monitoring | Risk for Individuals* | | | | x | x |
| SI-5 | **Security Alerts, Advisories, and Directives** | x | | x | x | x |
| SI-7 | **Software, Firmware, and Information Integrity** | | x | | x | x |
| SI-7(14) | *Software, Firmware, and Information Integrity | Binary or Machine Executable Code* | | | | x | x |
| SI-7(15) | *Software, Firmware, and Information Integrity | Code Authentication* | | | | | x |
| SI-12 | **Information Management and Retention** | x | | | | x |
| SI-20 | **Tainting** | | x | | x | x |
| SR-1 | **Policy and Procedures** | x | | x | x | x |
| SR-2 | **Supply Chain Risk Management Plan** | x | | | | x |
| SR-3 | **Supply Chain Controls and Processes** | x | | x | x | x |
| SR-3(1) | *Supply Chain Controls and Processes | Diverse Supply Base* | | | | x | x |
| SR-3(3) | *Supply Chain Controls and Processes | Sub-tier Flow Down* | | x | | x | x |
| SR-4 | **Provenance** | | | | x | x |
| SR-5 | **Acquisition Strategies, Tools, and Methods** | x | | x | x | x |
| SR-6 | **Supplier Assessments and Reviews** | | | | x | x |
| SR-7 | **Supply Chain Operations Security** | | | | x | x |
| SR-8 | **Notification Agreements** | x | | | x | x |
| SR-9 | **Tamper Resistance and Detection** | | | | x | x |
| SR-10 | **Inspection of Systems or Components** | x | x | | x | x |
| SR-11 | **Component Authenticity** | x | | x | x | x |
| SR-11(1) | *Component Authenticity | Anti-counterfeit Training* | x | | | x | x |
| SR-11(2) | *Component Authenticity | Configuration Control for Component Service and Repair* | x | | | x | x |
| SR-11(3) | *Component Authenticity | Anti-counterfeit Scanning* | | | | x | x |
| SR-12 | **Component Disposal** | x | | | x | x |
| SR-13 | **Supplier Inventory** | | | | x | x |

5674
5675

5676

## APPENDIX B: RISK EXPOSURE FRAMEWORK

There are numerous opportunities for vulnerabilities that impact the enterprise environment or the system/element to be intentionally or unintentionally inserted, created, or exploited throughout the supply chain. Exploitation of these vulnerabilities is known as a supply chain threat event. **A Threat Scenario is a set of discrete threat events, associated with a specific potential or identified existing threat source or multiple threat sources, partially ordered in time.** Developing and analyzing threat scenarios can help organizations have a more comprehensive understanding of the various types of threat events that can occur and lay the ground work for analyzing the likelihood and impact a specific event or events would have on an organization.  Conducting this analysis is a useful way to discover gaps in controls and to identify and prioritize appropriate mitigating strategies.[19]

Threat scenarios are generally used in two ways:

- To translate the often disconnected information garnered from a risk assessment, such as described in [NIST SP 800-30 Rev. 1] , into a more narrowly scoped and tangible, story-like situation for further evaluation. These stories can help organizations to discover dependencies and additional vulnerabilities requiring mitigation and used for training; and

- To determine the impact that the successful exercise of a specific vulnerability would have on the organization and identify the benefits of mitigating strategies.

Threat scenarios serve as a key component of the organization's cyber supply chain risk management process described in Appendix C of this publication. An organization forms a threat scenario to analyze a disparate set of threat and vulnerability conditions to assemble a cohesive story that can be analyzed as part of a risk assessment. With a threat scenario defined, the organization can complete a risk assessment to understand how likely the scenario is and what would happen (i.e., the impact) as a result. Ultimately the analyzed components of a threat scenario are used to reach a risk determination which represents the organization's conclusion on its level of exposure to a cyber supply chain risk.

Once a risk determination has been made – the organization will determine a path for responding to the risk using the Risk Exposure Framework. Within the Risk Exposure Framework – organizations will document the threat scenario, the risk analysis, as well as the identified a risk response strategy and any associated C-SCRM controls.

This appendix provides an example of a Risk Exposure Framework for C-SCRM that can be used by organizations to develop their own, tailored Risk Exposure Framework for potential and identified threats that best suits their needs. It contains five examples of how this framework may be used. The examples differ slightly in their implementation of the framework so as to show how the framework may be tailored by an organization. Each example identifies one or more vulnerabilities, describes a specific threat source, identifies the expected impact on the organization, and proposes SP 800-161, Rev. 1 C-SCRM controls that would help mitigate the resulting risk.

---

[19] Additional example threat scenarios and threat lists can be found in the ICT SCRM Task Force: Threat Scenarios Report, February 2021, https://www.cisa.gov/publication/ict-scrm-task-force-threat-scenarios-report.  This report leveraged the 2015 version of the NIST SP 800-161.

RISK EXPOSURE FRAMEWORK

**Step 1: Create a Plan for Developing and Analyzing Threat Scenarios**

- Identify the purpose of the threat scenario analysis in terms of the objectives, milestones, and expected deliverables;
- Identify the scope of organizational applicability, level of detail, and other constraints;
- Identify resources to be used, including personnel, time, and equipment; and
- Define a Risk Exposure Framework to be used for analyzing scenarios.

**Step 2: Characterize the Environment**

- Identify core mission/business processes and key organizational dependencies;
- Describe threat sources that are relevant to the organization. Include the motivation and resources available to the threat source, if applicable;
- List known vulnerabilities or areas of concern (Note: Examples of areas of concern include the planned outsourcing of a manufacturing plant, the pending termination of a maintenance contract, or the discontinued manufacture of an element.);
- Identify existing and planned controls;
- Identify related regulations, standards, policies, and procedures; and
- Define an acceptable level of risk (risk threshold) per the organization's assessment of Tactics, Techniques, and Procedures (TTPs), system criticality, and a risk owner's set of mission or business priorities. The level of risk or risk threshold can be periodically revisited and adjusted to reflect the elasticity of the global supply chain, organizational changes, and new mission priorities.

**Step 3: Develop and Select Threat Event(s) for Analysis**

- List possible ways threat sources could exploit known vulnerabilities or impact areas of concern to create a list of events (Note: Historical data is useful in determine this information.);
- Briefly outline the series of consequences that could occur as a result of each threat event. These may be as broad or specific as necessary. If applicable, estimate the likelihood and impact of each event;
- Eliminate those events that are clearly outside the defined purpose and scope of the analysis;
- Describe in more detail the remaining potential threat events. Include the TTPs a threat source may use to carry out attacks (Note: The level of detail in the description is dependent on the needs of the organization.); and
- Select for analysis those events that best fit the defined purpose and scope of the analysis. More likely or impactful events, areas of concern to the organization, and an event that can represent several of the other listed events are generally useful candidates.

**Step 4: Conduct an Analysis using the Risk Exposure Framework**

- For each threat event, note any immediate consequences of the event and identify those organizational units and processes that would be affected, taking into account existing and planned controls and the extent to which those controls are able to effectively prevent, withstand, or otherwise mitigate the harm that could result from the threat event, and applicable regulations, standards, policies, and procedures;
- Estimate the impact these consequences would have on the mission/business processes, information, assets, as well as the organizational units or other stakeholders affected, preferably in quantitative terms from historical data and taking into account existing and planned controls, and applicable regulations, standards, policies, and procedures (Note: It may be beneficial to identify a "most likely" impact level and a "worst-case" or "100-year" impact level.); and

5767    • Identify those organizational units, processes, information (access or flows), and/or assets that
5768      may or would be subsequently affected, the consequences and the impact levels, until each
5769      affected critical affected items has been analyzed, taking into account existing and planned
5770      controls, and applicable regulations, standards, policies, and procedures (e.g., If a critical server
5771      goes down, one of the first processes affected may be the technology support department, but if
5772      they determine a new part is needed to bring the server backup, the procurement department may
5773      become involved.).
5774
5775    **Step 5: Determine C-SCRM Applicable Controls**
5776    • Determine if and which threat scenario events create a risk level that exceeds a risk owner's
5777      acceptable level of risk (risk threshold). (Note: In some cases, the level of acceptable risk may be
5778      dependent on the capability to implement, or the cost of, mitigating strategies.) Identify
5779      opportunities to strengthen existing controls or potential new mitigating controls. Using a list of
5780      standard or recommended controls can make this process simpler. This appendix uses the controls
5781      in Section 4 of NIST SP 800-161 Rev. 1.
5782    • Estimate the effectiveness of existing and planned controls at reducing the risk of a scenario;
5783    • Estimate the capability and resources needed (in terms of money, personnel, time) to implement
5784      potential new or strengthened controls; and
5785    • Identify those C-SCRM controls or combinations of C-SCRM controls that could cause the
5786      estimated residual risk of a threat event to drop to an acceptable level in the most resource-
5787      effective manner, taking into account any rules or regulations that may apply (Note:
5788      Consideration should be given to the potential that one control will help mitigate the risk from
5789      more than one event, or that a control may increase the risk of a separate event.).
5790
5791    **Step 6: Evaluate / Feedback**
5792    • Develop a plan to implement the selected controls and evaluate their effectiveness; and
5793    • Evaluate the effectiveness of the Risk Exposure Framework and make improvements as needed.
5794
5795

5796
5797

**Table B-1: Sample Risk Exposure Framework**

| Threat Scenario | Threat | |
|---|---|---|
| | **Threat Event Description** | *Describe possible ways threat sources could exploit known vulnerabilities or impact areas of concern to create a list of events.*<br><br>Threat event: An event or situation that has the potential for causing undesirable consequences or impact. |
| | **Threat Event Outcome** | *Describe the outcome of the threat event.*<br><br>Threat Event Outcome:  The effect a threat acting upon a vulnerability has on the confidentiality, integrity, and/or availability of the organization's operations, assets, and/or individuals. |
| **Organizational units / processes/information/ assets/stakeholders affected** | | *List the affected organizational units / processes/information/ assets/stakeholders affected.* |
| | **Impact** | *Enter the estimate of the impact the outcome of the consequences would have on the mission/business processes, information, assets, as well as the organizational units or other stakeholders affected, preferably in quantitative terms from historical data and taking into account existing and planned controls, and applicable regulations, standards, policies, and procedures (Note: It may be beneficial to identify a "most likely" impact level and a "worst-case" or "100-year" impact level.)*<br><br>The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. |
| | **Likelihood** | *Enter the likelihood a specific event or events would have on an organization*<br><br>Likelihood: Chance of something happening |
| | **Risk Score (Impact x Likelihood)** | *Enter the risk score by multiplying impact x likelihood.*<br><br>*A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.* |
| | **Acceptable Level of Risk** | *Define an acceptable level of risk (risk threshold) per the organization's assessment of Tactics, Techniques, and Procedures (TTPs), system criticality, risk appetite and tolerance, and a risk owner's set strategic goals and objectives.*<br><br>Acceptable Risk:  A level of residual risk to the organization's operations, assets, or individuals that falls within the defined risk appetite and risk tolerance thresholds set by the organization. |
| Risk Mitigation | **Potential Mitigating Strategies / C-SCRM Controls** | *List the potential mitigating risk strategies and any relevant C-SCRM controls.* |

151

| | | |
|---|---|---|
| | | C-SCRM Risk Mitigation: A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the cyber supply chain risks presented by the supplier, the supplied products and services, or the supply chain. |
| | **Estimated Cost of Mitigating Strategies** | *Enter estimated cost of risk mitigating strategies.* |
| | **Change in Likelihood** | *Identify potential changes in likelihood.* |
| | **Change in Impact** | *Identify potential changes in impact.* |
| | **Selected Strategies** | *List selected strategies to reduce impact.* |
| | **Estimated Residual Risk** | *Enter the estimated amount of residual risk*<br><br>Residual Risk:  Portion of risk remaining after security measures have been applied. |

5798
5799

## SAMPLE SCENARIOS

This appendix provides five example threat scenarios specific to the U.S. government using a fictitious 'ABC Company' and the Risk Exposure Framework described above. The examples purposely vary in level of specificity and detail to show that threat scenarios can be as broad or specific—as detailed or generic—as necessary. While these scenarios use percentages and basic scoring measures (High, Moderate, Low) for likelihood, impact, and risk, organizations may use any number of different units of measure (e.g., CVSS score, etc.). Additionally, these scenarios vary slightly in implementation of the risk response framework to show the Risk Exposure Framework can be adapted as needed.

### SCENARIO 1: Influence or Control by Foreign Governments Over Suppliers[20]

### Background

An organization has decided to perform a threat scenario analysis of its Printed Circuit Board (PCB) suppliers. The scenario will focus on the sensitivity of the business to unforeseen fluctuations in component costs.

### Threat Source

ABC Company designs, assembles, and ships 3.5 million personal computers per year. It has a global footprint both in terms of customer and supply bases. Five years ago, in an effort to reduce the cost of goods sold, ABC Company shifted a majority of its PCB procurement to Southeast Asia. To avoid being single sourced, ABC Company finalized agreements with five different suppliers within the country and has enjoyed a positive partnership with each during this time.

### Vulnerability

N/A

### Threat Event Description

The organization has established the following fictitious threat for the analysis exercise: Last year, the country where ABC Company does most of their PCB business has seen a new regime take over the government. This regime has been more focused on improving finances and business environment within the country, allowing larger firms who set up headquarters and other major centers within country advantages to more easily and cost-efficiently do business with suppliers within the same region. In February of 2019, this now-corrupt regime has passed new legislation establishing an additional 20 percent tax on all electronic components and goods sold outside of the country. This new law was to take effect on June 1, 2019.

When the new law was announced, the current ABC Company inventory of PCBs was about 10 percent of yearly demand, which was the typical inventory level with which they were comfortable. Before June, ABC Company reached out to all five suppliers to order additional materials, but there was quickly a shortage due to higher demand from many foreign customers of these products. By June 1, the day the

---

5845    new tax law took effect, ABC Company had reached an inventory level of up to 15 percent of yearly
5846    demand.
5847
5848    **Outcome**
5849
5850    Between February and June, ABC Company also looked to partner with new suppliers, but there were
5851    several issues identified. One in every 10 new suppliers ABC Company reached out to required a lead
5852    time for ramping up to desired demand of anywhere from 6 months to 18 months. This would necessitate
5853    additional work on ABC Company's part, including testing samples of the supplier PCBs and finalizing
5854    logistical details, to monitoring supplier-side activities such as procurement of raw materials and
5855    acquisition of additional personnel, production space, etc. necessary to meet the new demand.
5856
5857    The second issue due to the current contracts with all five current suppliers in Southeast Asia involved
5858    meeting minimum demand requirements, in that ABC Company was committed to purchasing at
5859    minimum 100,000 PCB's per month for the duration of the contracts (which ranged anywhere from 3
5860    months to 24 months in length). This would mean ABC Company could not easily avoid the cost
5861    implications of the new tax. Could ABC Company absorb the cost of the PCBs? With a 20 percent cost
5862    increase, this eroded the margins of a PC from 13.5 percent down to 4.5 percent on average. For some of
5863    the lower-margin ABC Company offerings, it would likely result in discontinuing the line and using the
5864    now more expensive PCB's on higher-end models that could carry more margin.
5865
5866    **Organizational Units / Processes Affected**
5867
5868    N/A
5869
5870    **Potential Mitigating Strategies / C-SCRM Controls**
5871
5872    Perform regular assessment and review of supplier risk[21]; Diversify suppliers not only by immediate
5873    location, but also by country, region and other factors; Build cost implications into supplier contracts,
5874    making it easier to part ways with suppliers when costs rise too high (whether by fault of the supplier or
5875    otherwise); Adjust desired inventory levels to better account for unexpected shortage of demand at critical
5876    times; and Employ more resources in countries or regions of key suppliers with the intent to source
5877    advanced notice of new legislature that may negatively affect business.
5878

---

[21] Regular assessment and review of supplier risk mitigating strategy was added to original Scenario 1 text from ICT SCRM Task Force: Threat
Scenarios Report, February 2021, https://www.cisa.gov/publication/ict-scrm-task-force-threat-scenarios-report.  This report leveraged the 2015
version of the NIST SP 800-161.

5879                                    **Table B-2: Scenario 1**

| | | |
|---|---|---|
| **Threat Scenario** | **Threat Source** | Dynamic geopolitical conditions that impact the supply of production components for PCs |
| | **Vulnerability** | Geographical concentration of suppliers for a key production component |
| | **Threat Event Description** | ABC Company shifted a majority of its Printed Circuit Board (PCB) procurement to Southeast Asia to reduce cost of goods sold. In an effort to avoid being single sourced, ABC Company finalized agreements with five different suppliers within the country.<br><br>The country in which ABC Company conducts most of their PCB business has seen a new regime assume governmental authority. In February of 2019, this now-corrupt regime passed legislation establishing an additional 20 percent tax on all electronic components and goods sold outside of the country. This law was to take effect on June 1, 2019.<br><br>When the new law was announced, the current ABC Company inventory of PCBs was about 10 percent of yearly demand, at the typical level of inventory with which they were comfortable. Before June, ABC Company reached out to all five suppliers to order additional materials, but there was quickly a shortage due to higher demand from many foreign customers of these products. By June 1, the day the new tax law took effect, ABC Company had reached an inventory level up to 15 percent of annual demand. |
| | **Threat Event Outcome** | ABC Company also looked to partner with new suppliers, but there were issues identified with this approach: 1) One out of every 10 new suppliers to which ABC Company reached out required a lead time to ramp up to desired demand of anywhere from 6 months to 18 months; and 2) Current contracts with all five active suppliers in Southeast Asia stipulated minimum demand requirements, meaning ABC Company was committed to purchasing a minimum of 100,000 PCB's per month for the duration of the contracts (which ranged anywhere from 3 months to 24 months in length). This would mean ABC Company could not easily avoid the cost implications of this new tax. With a 20 percent cost increase, the margins of a PC eroded from 13.5 percent to 4.5 percent, on average. |
| | **Organizational units / processes affected** | N/A |
| **Risk** | **Impact** | High: $40,000,000 decline in PC product line profit |
| | **Likelihood** | Moderate: 10% annualized probability of occurrence |
| | **Risk Score (Impact x Likelihood)** | High: Inherent Risk Exposure equal to approx. $4,000,000 in product line profit |
| | **Acceptable Level of Risk** | No greater than 10% probability of greater than $10,000,000 in product line profit |
| **Mitig...** | **Potential Mitigating Strategies / C-SCRM Controls** | Assess and review supplier risk to include FOCI [SR-6(1)], employ supplier diversity requirements [C- | Perform regular assessment and review of supplier risk; Diversify suppliers not just by immediate |

| | SCRM_PL-3(1)], employ supplier diversity [SCRM_PL-8(2)], and adjust inventory levels [CM-8] | location, but by country, region and other factors; Build cost implications into supplier contracts, making it easier to walk away from suppliers when costs rise too high (whether its fault of the supplier or not); Adjust desired inventory levels to better account for unexpected shortage of demand at critical times; and Employ more resources in countries or regions of key suppliers with the intent to source advanced notice of new legislature that may negatively affect business. |
|---|---|---|
| **Estimated Cost of Mitigating Strategies** | N/A | |
| **Change in Likelihood** | Low: 10% probability of occurrence | |
| **Change in Impact** | Moderate: $2,000,000 in product line profit | |
| **Selected Strategies** | Combination of strategies using the mitigation noted. | |
| **Estimated Residual Risk** | Low: Residual risk exposure 0.02% of PC product line profit margin | |

### *SCENARIO 2: Telecommunications Counterfeits*

### Background

A large organization, ABC Company, has developed a system that is maintained by contract with an external integration company. The system requires a common telecommunications element that is no longer available from the Original Equipment Manufacturer (OEM). The OEM has offered a newer product as a replacement which would require modifications to the system at a cost of approximately $1 million. If the element is not upgraded, the agency and system integrator would have to rely on secondary market suppliers for replacements. The newer product provides no significant improvement on the element currently being used.

ABC Company has decided to perform a threat scenario analysis to determine whether to modify the system to accept the new product or accept the risk of continuing to use a product that is no longer in production.

### Environment

The environment is characterized as follows:
- The system is expected to last ten more years without any major upgrades/modifications and has a 99.9% uptime requirement.

- Over 1000 of the $200 elements are used throughout the system and approximately 10% are replaced every year due to regular wear-and-tear, malfunctions, or other reasons. The integrator has an approximate three-month supply on hand at any given time.
- The element is continuously monitored for functionality, and efficient procedures exist to reroute traffic and replace the element should it unexpectedly fail.
- Outages resulting from unexpected failure of the element are rare, localized, and last only a few minutes. More frequently, when an element fails, the system's functionality is severely reduced for approximately one to four hours while the problem is diagnosed and fixed or the element replaced.
- Products such as the element in question have been a common target for counterfeiting.
- The integrator has policies restricting the purchase of counterfeit goods and a procedure to follow if a counterfeit is discovered [Ref. SR-11].
- The integrator and acquiring agency have limited testing procedures to ensure functionality of the element before acceptance [Ref. SR-5(2)].

**Threat Event**

To support the threat scenario, the agency created a fictitious threat source described as a group motivated by profit with vast experience creating counterfeit solutions. The counterfeiter is able to make a high profit margin by creating and selling as genuine products that are visually identical to their genuine counterparts but which use lower-quality materials. They have the resources to copy most trademark and other identifying characteristics and insert counterfeits into a supply chain commonly used by the organization with little to no risk of detection. The counterfeit product is appealing to unaware purchasing authorities as it is generally offered at a discount, sold as excess inventory or as stockpile.

If an inferior quality element was inserted into the system, it would likely fail more often than expected, causing reduced functionality of the system. In the event of a large number of counterfeit products integrating with genuine parts into the system randomly, the number and severity of unexpected outages could grow significantly. The agency and integrator decided that the chances a counterfeit product could be purchased to maintain the system and the estimated potential impact of such an event were high enough to warrant further evaluation.

**Threat Scenario Analysis**

The person(s) purchasing the element from a supplier will be the first affected by a counterfeit product. Policy requires they attempt to purchase a genuine product from vetted suppliers. This individual would have to be led to believe that the product is genuine. As the counterfeit product in question is visually identical to the element desired, and at a discount, there is a high chance the counterfeit will be purchased. One will be tested to ensure functionality, and then the items will be placed into storage.

When one of the elements in the system needs replacing, an engineer will install a counterfeit, quickly test to ensure it is running properly, and record the change. It could take two years for the counterfeit product to fail, so up to 200 counterfeit elements could be inserted into the system before the first sign of failure. If all the regularly replaced elements are substituted for counterfeits and each counterfeit fails after two years, the cost of the system would increase by $160,000 in ten years. The requisite maintenance time would also cost the integration company in personnel and other expenses.

When a counterfeit fails, it will take approximately one to four hours to diagnose and replace the element. During this time, productivity is severely reduced. If more than one of the elements fails at the same time, the system could fail entirely. This could cause significant damage to agency operations and violate the

5953    99.9% uptime requirements set forth in the contract. Plus, if it becomes determined that the element failed
5954    because it was counterfeit, additional costs associated with reporting the counterfeit would be incurred.
5955
5956    **Mitigation Strategy**
5957
5958    The following were identified as potential mitigating activities (from NIST SP 800-161 Rev. 1):
5959
5960    - Require developers to perform security testing/evaluation at all post-design phases of the SDLC
5961      [Ref. SA-11];
5962    - Validate that the information system or system component received is genuine and has not been
5963      altered [Ref. SR-11];
5964    - Incorporate security requirements into the design of information systems (security engineering)
5965      [Ref. PL-8, SC-36]; and
5966    - Employ supplier diversity requirements [PL-8(2)].
5967
5968    Based on these controls, the agency was able to devise a strategy that would include:
5969
5970    - Acceptance testing: Examination of elements to ensure they are new, genuine, and that all
5971      associated licenses are valid. Testing methods include, where appropriate: physical inspection by
5972      trained personnel using digital imaging, digital signature verification, serial/part number
5973      verification, and sample electrical testing;
5974    - Increasing security requirements into the design of the system by adding redundant elements
5975      along more critical paths (as determined by a criticality analysis) and in order to minimize the
5976      impact of an element failure; and
5977    - Search for alternative vetted suppliers/trusted components.
5978
5979    It was determined that this strategy would cost less than accepting the risk of allowing counterfeits into
5980    the system or modifying the system to accept the upgraded element. The estimated cost for implementing
5981    a more rigorous acquisition and testing program was $80,000; the cost for increasing security engineering
5982    requirements was $100,000.
5983
5984                                     **Table B-3: Scenario 2**
5985

| Threat Scenario | Threat Source | Counterfeit telecommunications element introduced into supply chain |
|---|---|---|
| | Vulnerability | Element no longer produced by OEM<br>Purchasing authorities unable / unwilling to identify and purchase only genuine elements |
| | Threat Event Description | Threat agent inserts their counterfeit element into a trusted distribution chain. → Purchasing authorities buy the counterfeit element. → Counterfeit elements installed into the system |
| | Threat Event Outcome | The element fails more frequently than before, increasing the number of outages |
| Organizational units / processes/information/ assets/stakeholders affected | | Acquisitions<br>Maintenance<br>OEM / supplier relations<br>Mission-essential functions |
| (Risk | Impact | Moderate: Element failure leads to 1-4-hour system downtime |

| | | | |
|---|---|---|---|
| | **Likelihood** | High: Significant motivation by threat actor and high vulnerability due to agency's inability to detect counterfeits with 25% annualized probability of premature component failure | |
| | **Risk Score (Impact x Likelihood)** | Medium: Significant short-term disruptions that lead downtime to exceed uptime threshold by 0.5% (e.g., 99.4% < 99.9% requirement) | |
| | **Acceptable Level of Risk** | Low: System must have less than 10% annualized probability of missing 99% uptime thresholds | |
| **Mitigation** | **Potential Mitigating Strategies / C-SCRM Controls** | Increase acceptance testing capabilities [C-SCRM_SA-9; C-SCRM_SA-10], increase security requirements in design of systems [C-SCRM_PL-2, and employ supplier diversity requirements [C-SCRM_PL-8(2)] | Modify the system to accept element upgrade |
| | **Estimated Cost of Mitigating Strategies** | $180,000 | $1 million |
| | **Change in Likelihood** | Low: 8% annualized probability of component failure | |
| | **Change in Impact** | Low: Element failure causes failover to redundant system component – cost limited to maintenance and replacement | |
| | **Selected Strategies** | Agency-level examination and testing<br>Place elements in escrow until they pass defined acceptance testing criteria<br>Increase security engineering<br>Search for multiple suppliers of the element | |
| | **Estimated Residual Risk** | Low: 8% annualized probability of component failures leading to system downtime (i.e., less than 99.9% uptime) | |

5986
5987
5988
5989  ***SCENARIO 3: Industrial Espionage***

5990
5991  **Background**

5992
5993  ABC Company, a semiconductor (SC) company used by the organization to produce military and
5994  aerospace systems, is considering a partnership with a KXY Co. to leverage their fabrication facility. This
5995  would represent a significant change in the supply chain related to a critical system element. A committee
5996  was formed including representatives from the organization, ABC Company, and the integration company
5997  to help identify the impact the partnership would have on the organization and risk-appropriate mitigating
5998  practices to enact when the partnership is completed.

5999
6000  **Environment**

6001
6002  The systems of concern are vital to the safety of military and aerospace missions. While not classified, the
6003  element that KXY would be expected to manufacture is unique, patented, and critical to the operational
6004  status of the systems. Loss of availability of the element while the system is operational could have
6005  significant, immediate impact across multiple agencies and the civilian populous, including loss of life

6006 and millions of dollars in damages. An initial Risk Assessment was accomplished using [NIST SP 800-30
6007 Rev. 1], and the existing level of risk for this is was given a score of "Moderate."
6008
6009 KXY currently produces a state-of-the-art, low-cost wafer fabrication with a primarily commercial focus.
6010 The nation-state in which KXY operates has a history of conducting industrial espionage to gain
6011 IP/technology. They have shown interest in semiconductor technology and provided a significant grant to
6012 KXY to expand into the military and aerospace markets. While KXY does not currently have the testing
6013 infrastructure to meet U.S. industry compliance requirements, the nation-state's resources are significant,
6014 including the ability to provide both concessions as well as incentives to help KXY meet those
6015 requirements.
6016
6017 The key area of concern was that the nation-state in which KXY operates would be able to use its
6018 influence to gain access to the element or the element's design.
6019
6020 The committee reviewed current mitigation strategies in place and determined that ABC Company, the
6021 integration company, and the organization had several existing practices to ensure that the system and all
6022 critical elements, as determined by a criticality analysis, met specific functionality requirements. For
6023 example, the system and critical elements are determined compliant with relevant industry standards. As
6024 part of their requirements under [NIST SP 800-53 Rev.5], the agency had some information protection
6025 requirements (Ref. PM-11). In addition, ABC Company had a sophisticated inventory tracking system
6026 that required that most elements to be uniquely tagged using RFID technology or otherwise identified for
6027 traceability (Ref. SR-4)).
6028
6029
6030 **Threat Scenario**
6031
6032 Based on past experience, the organization decided that KXY's host nation would likely perform one of
6033 two actions if given access to the technology: sell it to interested parties, or insert/identify vulnerabilities
6034 for later exploitation. For either of these threat events to succeed, the host nation would have to
6035 understand the purpose of the element and be given significant access to the element or element's design.
6036 This could be done with cooperation of KXY's human resources department, through deception, or by
6037 physical or electronic theft. Physical theft would be difficult given existing physical control requirements
6038 and inventory control procedures. For a modified element to be purchased and integrated with the system,
6039 it would need to pass various testing procedures at both the integrator and agency levels. Testing methods
6040 currently utilized included radiographic examination, material analysis, electrical testing, and sample
6041 accelerated life testing. Modifications to identification labels/schemes would need to be undetectable in a
6042 basic examination. In addition, KXY would need to pass routine audits, which would check KXY's
6043 processes for ensuring the quality and functionality of the element.
6044
6045 The committee decided that, despite existing practices, there was a 30% chance that the host nation would
6046 have the motivation and ability to develop harmful modifications to the element without detection, exploit
6047 previously unknown vulnerabilities, or provide the means for one of their allies to do the same. This could
6048 result in a loss of availability or integrity of the system, causing significant harm. Using information from
6049 an initial Risk Assessment accomplished using [NIST SP 800-30 Rev. 1], the committee identified this as
6050 the worst-case scenario with an impact score of "High."
6051
6052 There is approximately a 40% chance that the host nation could and would sell the technology to
6053 interested parties, resulting in a loss of technological superiority. If this scenario occurred, friendly
6054 military and civilian lives could be at risk, intelligence operations would be damaged, and more money

would be required to invest in a new solution. The committee assigned an impact score for this scenario of "Moderate."

The committee determined that the overall combined risk score for the vulnerability of concern was "High."

**Mitigating Strategies**

Using NIST SP 800-161 Rev. 1 as a base, three broad strategies were identified by the committee: (1) improve traceability capabilities, (2) increase provenance and information requirements, and (3) choose another supplier. These three options were analyzed in more detail to determine specific implementation strategies, their impact on the scenarios, and their estimated cost to implement. (Specific technologies and techniques are not described in this case but would be useful in an actual threat scenario evaluation).

Improve traceability and monitoring capabilities
- CM-8 - SYSTEM COMPONENT INVENTORY
- IA-1 - POLICY AND PROCEDURES
- SA-10 - DEVELOPER CONFIGURATION MANAGEMENT
- SR-8 - NOTIFICATION AGREEMENTS
- SR-4 - PROVENANCE

Cost = 20 % increase
Impact = 10 % decrease

Increase provenance and information control requirements
- AC-21 - INFORMATION SHARING
- SR-4 - PROVENANCE

Cost = 20 % increase
Impact = 20 % decrease

Choose another supplier
- SR-6- SUPPLIER ASSESSMENTS AND REVIEWS

Cost = 40 % increase
Impact = 80 % decrease

Based on this analysis, the committee decided to implement a combination of practices:
- Develop and require unique, difficult-to-copy labels or alter labels to discourage cloning or modification of the component [Ref. SR-3(2)];
- Minimize the amount of information that is shared to suppliers. Require that the information be secured [Ref. AC-21]; and
- Require provenance be kept and updated throughout the SDLC [Ref. SR-4].

With this combination of controls, the estimated residual risk was determined to be equivalent with the existing risk without the partnership at a cost increase that is less than if the organization had changed suppliers.

6100

**Table B-4: Scenario 3**

6101

| | | | | |
|---|---|---|---|---|
| **Threat Scenario** | **Threat Source** | Nation-state with significant resources looking to steal IP | | |
| | **Vulnerability** | Supplier considering partnership with company that has relationship with threat source | | |
| | **Threat Event Description** | Nation-state helps KXY meet industry compliance requirements. <br> ABC Company partners with KXY to develop chips | | |
| | **Existing Practices** | Strong contractual requirements as to the functionality of the system and elements <br> Comprehensive inventory tracking system at ABC Company <br> Industry compliance requirements | | |
| | **Threat Event Outcome** | Nation-state extracts technology threat actor, modifies technology, or exploits previously unknown vulnerability | | |
| **Organizational units / processes/information/ assets/stakeholders affected** | | KXY Supplier <br> ABC Company integrator functionality testing <br> Technology users <br> Other federal agencies / customers | | |
| **Risk** | **Impact** | Technology modified / vulnerabilities exploited – High | Technology sold to interested parties – Moderate | |
| | **Likelihood** | Moderate | Moderate | |
| | **Risk Score (Impact x Likelihood)** | High | | |
| | **Acceptable Level of Risk** | Moderate | | |
| **Mitigation** | **Potential Mitigating Strategies / C-SCRM Controls** | **(1) Improve traceability and monitoring capabilities** | **(2) Increase provenance and information control requirements** | **(3) Choose another supplier** |
| | **Estimated Cost of Mitigating Strategies** | 20% increase | 20% increase | 40% increase |
| | **Change in Likelihood** | Moderate → Low | | |
| | **Change in Impact** | High → Moderate | | |
| | **Selected Strategies** | Develop and require unique, difficult-to-copy labels or alter labels to discourage cloning or modification of the component [C-SCRM_PE-3] <br> Minimize the amount of information that is shared to suppliers. Require that the information be secured [C-SCRM AC-21] <br> Require provenance be kept and updated throughout the SDLC [C-SCRM_SR-4] | | |
| | **Estimated Residual Risk** | Moderate – The residual risk was determined to be equivalent with the existing risk without the partnership | | |

6102
6103

***SCENARIO 4: Malicious Code Insertion***

**Background**

ABC Company has decided to perform a threat scenario analysis on a traffic control system. The scenario is to focus on software vulnerabilities and should provide general recommendations regarding mitigating practices.

**Environment**

The system runs nearly automatically and uses computers running a commonly available operating system along with centralized servers. The software was created in-house and is regularly maintained and updated by an integration company on contract for the next five years. The integration company is large, frequently used by ABC Company in a variety of projects, and has significant resources to ensure that the system maintains its high availability and integrity requirements.

Threats to the system could include loss of power to the system, loss of functionality, or loss of integrity causing incorrect commands to be processed. Some threat sources could include nature, malicious outsiders, and malicious insiders. The system is equipped with certain safety controls such as backup generator power, redundancy of design, and contingency plans if the system fails.

**Threat Event**

ABC Company decided that the most concerning threat event would result from a malicious insider compromising the integrity of the system. Possible attacks could include the threat actor inserting a worm or a virus into the system, reducing its ability to function, or they could manually control the system from one of the central servers or by creating a back-door in the server to be accessed remotely. Depending on the skillfulness of the attack, an insider could gain control of the system, override certain fail-safes, and cause significant damage.

Based on this information, ABC Company developed the following fictitious threat event for analysis:

> *John Poindexter, a disgruntled employee of the integration company, decides to insert some*
> *open source malware into a component of the system. He then resigns from the firm, leaving no*
> *traceability of his work. The malware has the ability to call home to John and provide him*
> *access to stop or allow network traffic at any or all 50 of the transportation stations. As a*
> *result, unpredictable, difficult-to-diagnose disruptions would occur, causing significant*
> *monetary losses and safety concerns.*

After a Risk Assessment was accomplished using [NIST SP 800-30 Rev. 1], management decided that the acceptable level of risk for this scenario was "Moderate."

**Threat Scenario Analysis**

If John were successful, a potential course of events could occur as follows:

> John conducts a trial run, shutting off the services of one station for a short time. It would be
> discounted as a fluke and have minimal impact. Later, John would create increasingly frequent
> disruptions at various stations. These disruptions would cause anger among employees and

6153    customers and some safety concerns. The integration company would be made aware of the
6154    problem and begin to investigate the cause. They would create a workaround, and make the
6155    assumption there was a bug in the system. However, because the malicious code would be buried
6156    and difficult to identify, the integration company wouldn't discover it. John would then create a
6157    major disruption across several transportation systems at once. The workaround created by the
6158    integration company would fail due to the size of the attack, and all transportation services would
6159    be halted. Travelers would be severely impacted, and the media alerted. The method of attack
6160    would be identified, and the system modified to prevent John from accessing the system again.
6161    However, the underlying malicious code would remain. Revenue would decrease significantly for
6162    several months. Legal questions would arise. Resources would be invested in assuring the public
6163    that the system was safe.

6164

## Mitigating Practices

6166

6167    ABC Company identified the following potential areas for improvement:

6168

6169    • Establish and retain identification of supply chain elements, processes, and actors [SR-4];
6170    • Control access and configuration changes within the SDLC and require periodic code reviews
6171      [AC-1, AC-2, CM-3];
6172    • Require static code testing [RA-9]; and
6173    • Incident Handling [IR-4].

6174
6175

6176                              **Table B-5: Scenario 4**

6177

| | | |
|---|---|---|
| **Threat Scenario** | **Threat Source** | Integrator– Malicious Code Insertion |
| | **Vulnerability** | Minimal oversight of integrator activities - no checks and balances for any individual inserting a small piece of code |
| | **Threat Event Description** | Disgruntled employee of an Integrator company inserts malicious functionality into traffic navigation software, and then leaves the ABC Company |
| | **Existing Practices** | Integrator: peer-review process<br>Acquirer: Contract that sets down time, cost, and functionality requirements |
| | **Threat Event Outcome** | 50 large metro locations and 500 instances affected by malware. When activated, the malware causes major disruptions to traffic |
| **Organizational units / processes/information/ assets/stakeholders affected** | | Traffic Navigation System<br>Implementation company<br>Legal<br>Public Affairs |
| **Risk** | **Impact** | High – Traffic disruptions are major and last for two weeks while a work-around is created. Malicious code is not discovered and remains a vulnerability |
| | **Likelihood** | High |
| | **Risk Score (Impact x Likelihood)** | High |

| | | |
|---|---|---|
| **Mitigation** | **Acceptable Level of Risk** | Moderate |
| | **Potential Mitigating Strategies / C-SCRM Controls** | C-SCRM_AC-1; C-SCRM_AC-2; C-SCRM_CM-3; C-SCRM_IR-2; C-SCRM_SA-10; C-SCRM_SA-11 |
| | **Estimated Cost of Mitigating Strategies** | $2.5 million |
| | **Change in Likelihood** | High → Low |
| | **Change in Impact** | High (no change) |
| | **Selected Strategies** | Combination of strategies using the mitigation noted |
| | **Estimated Residual Risk** | Moderate |

6178
6179
6180    ### SCENARIO 5: Unintentional Compromise

6181
6182    ## Background

6183
6184    Uninformed insiders replace components with more cost-efficient solutions without understanding the
6185    implications to performance, safety, and long-term costs.

6186
6187    ABC Company has concerns about its acquisition policies and has decided to conduct a threat scenario
6188    analysis to identify applicable mitigating practices. Any practices selected must be applicable to a variety
6189    of projects and have significant success within a year.

6190
6191    ## Environment

6192
6193    ABC Company acquires many different systems with varying degrees of requirements. Because of the
6194    complexity of the environment, ABC Company officials decide they should use a scenario based on an
6195    actual past event.

6196
6197    ## Threat Event

6198
6199    Using an actual event as a basis, the agency designs the following threat event narrative:

6200
6201        Gill, a newly hired program manager, is tasked with reducing the cost of a $5 million system
6202        being purchased to support complex research applications in a unique physical environment. The
6203        system would be responsible for relaying information regarding temperature, humidity, and toxic
6204        chemical detection as well as storing and analyzing various data sets. There must not be any
6205        unscheduled outages more than 10 seconds long, or serious safety concerns and potential
6206        destruction of research will occur. ABC Company's threat assessment committee determined that
6207        the acceptable level of risk for this type of event has a score of 2/10.

165

Gill sees that a number of components in the system design are priced high compared with similar components he has purchased in the commercial acquisition space. Gill asks John, a junior engineer with the integration company, to replace several load balancer/routers in the system design to save costs.

**Threat Scenario Analysis**

ABC Company decides that there were three potential outcomes to the scenario:
1. It is determined that the modifications are inadequate before any are purchased (30 % chance, no impact);
2. It is determined that the modifications are inadequate during testing (40 % chance, low impact); or
3. The inadequacy of the modifications is undetected, the routers are installed in the system, begin to fail, and create denial of service incidents (30 % chance, high impact).


**Mitigating Strategies**

Three potential mitigating strategies were identified:
- Improve the existing training program [Ref. AT-1] and add configuration management controls to monitor all proposed changes to critical systems [Ref. CM-1];
- Improve the testing requirements [Ref. SA-11]; and
- Require redundancy and heterogeneity in the design of systems [Ref. SC-29, SC-36].

Adding configuration management controls would increase the likelihood that the modifications were rejected either at the initial stage or during testing, but it was determined that a $200,000 investment in training alone could not bring the level of risk to an acceptable level in the time required.

Improving the testing requirements would increase the likelihood of the modifications being rejected during testing, but it was determined that no amount of testing alone could bring the level of risk to an acceptable level.

Requiring redundancy and heterogeneity in the design of the system would significantly reduce the impact of this and other events of concern, but could double the cost of a project. In this scenario, it was determined that an investment of $2 million would be required to bring the risk to an acceptable level.

As a result of this analysis, ABC Company decides to implement a combination of practices:
- A mandatory, day-long training program for those handling the acquisition of critical systems and adding configuration management controls requiring changes be approved by a configuration management board (CMB) ($80,000 initial investment);
- $60,000 investment in testing equipment and software for critical systems and elements; and
- Redundancy and diversity of design requirements as deemed appropriate for each project.

It was determined that this combination of practices would be most cost-effective for a variety of projects and help mitigate the risk from a variety of threats.

6255

**Table B-6: Scenario 5**

<table>
<tr><td rowspan="6">Threat Scenario</td><td>**Threat Source**</td><td colspan="3">Internal Employee – Unintentional Compromise</td></tr>
<tr><td>**Vulnerability**</td><td colspan="3">Lax training practices</td></tr>
<tr><td>**Threat Event Description**</td><td colspan="3">A new acquisition officer (AO) with experience in commercial acquisition is tasked with reducing hardware costs. The AO sees that a number of components are priced high and works with an engineer to change the purchase order</td></tr>
<tr><td>**Existing Practices**</td><td colspan="3">Minimal training program that is not considered mandatory<br>Basic testing requirements for system components</td></tr>
<tr><td>**Threat Event Outcome**</td><td>Change is found unsuitable before purchase</td><td>Change is found unsuitable in testing</td><td>Change passes testing, routers installed and start to fail, causing a denial of service situation</td></tr>
<tr><td>**Organizational units / processes/information/ assets/stakeholders affected**</td><td>None</td><td>Acquisitions</td><td>Acquisitions, System, Users</td></tr>
<tr><td rowspan="4">Risk</td><td>**Impact**</td><td>None</td><td>Low</td><td>High</td></tr>
<tr><td>**Likelihood**</td><td>Moderate: 30%</td><td>High: 40 %</td><td>Moderate: 30 %</td></tr>
<tr><td>**Risk Score (Impact x Likelihood)**</td><td>None</td><td>Moderate</td><td>Moderate</td></tr>
<tr><td>**Acceptable Level of Risk**</td><td>Low</td><td>Moderate</td><td>High</td></tr>
<tr><td rowspan="8">Mitigation</td><td>**Potential Mitigating Strategies / SCRM Controls**</td><td>Improve training program and require changes be approved by CMB.</td><td>Improve acquisition testing</td><td>Improve design of system</td></tr>
<tr><td>**Estimated Cost of Mitigating Strategies**</td><td>$200,000</td><td>---</td><td>$2 million</td></tr>
<tr><td>**Change in Impact**</td><td>None – No Change</td><td>Low – No Change</td><td>High → Low</td></tr>
<tr><td>**Change in Likelihood**</td><td>30% →10%</td><td>40% →20%</td><td>30% -- No Change</td></tr>
<tr><td>**New Risk Score**</td><td>None</td><td>Low</td><td>Moderate</td></tr>
<tr><td>**Selected Strategies**</td><td colspan="3">Require mandatory training for those working on critical systems and require approval of changes to critical systems by a configuration management board (Cost = $100,000)</td></tr>
<tr><td>**Residual Risk:**</td><td colspan="3">Low</td></tr>
</table>

6256 **APPENDIX C: C-SCRM ACTIVITIES IN THE RISK MANAGEMENT PROCESS**

6257 Risk management is a comprehensive process that requires organizations to: (i) frame risk (i.e.,
6258 establish the context for risk-based decisions); (ii) assess risk; (iii) respond to risk once
6259 determined; and (iv) monitor risk on an ongoing basis using effective organizational
6260 communications and a feedback loop for continuous improvement in the risk-related activities of
6261 organizations. Figure 2-3 depicts interrelationships among the risk management process steps,
6262 including the order in which each analysis may be executed, and the interactions required to
6263 ensure that the analysis is inclusive of the various inputs at the organization, mission, and
6264 operations levels.
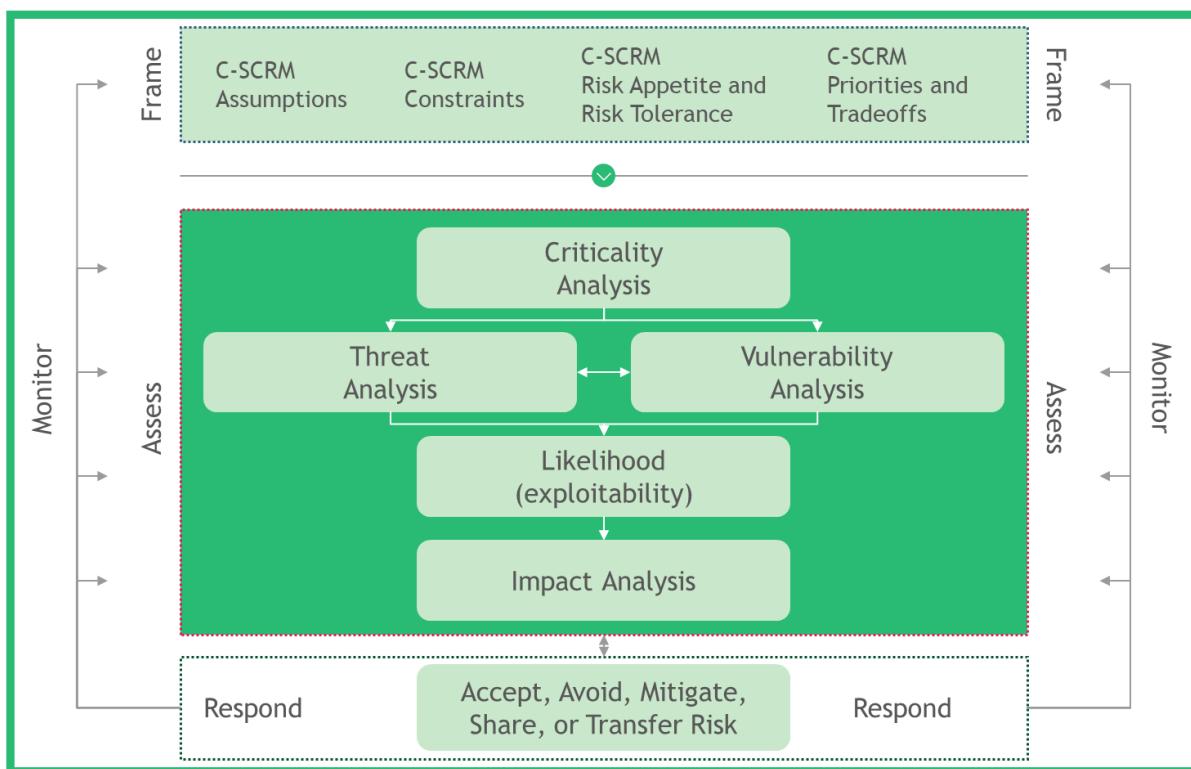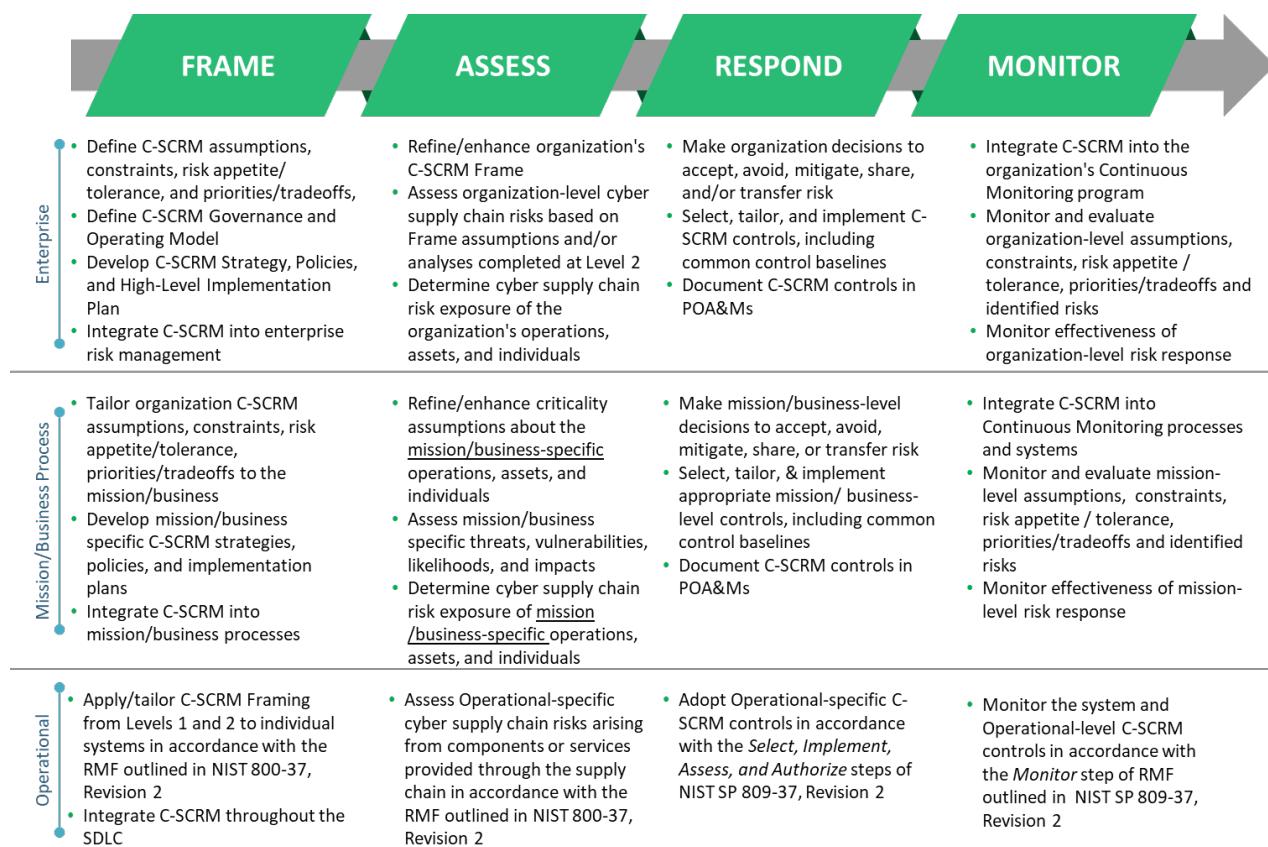


6265
6266                    **Fig. C-1: Cyber Supply Chain Risk Management (C-SCRM)**

6267 The steps in the risk management process (Frame, Assess, Respond, and Monitor) are iterative
6268 and not inherently sequential in nature. Different individuals may be required to perform the
6269 steps at the same time depending on a particular need or situation. Organizations have significant
6270 flexibility in how the risk management steps are performed (e.g., sequence, degree of rigor,
6271 formality, and thoroughness of application) and in how the results of each step are captured and
6272 shared—both internally and externally. The outputs from a particular risk management step will
6273 directly impact one or more of the other risk management steps in the risk management process.
6274
6275 Figure C-2 summarizes C-SCRM activities throughout the risk management process as they are
6276 performed within the three risk framework levels. The arrows between different steps of the risk
6277 management process depict simultaneous flow of information and guidance among the steps.
6278 Together the arrows indicate that the inputs, activities, and outputs are continuously interacting
6279 and influencing one another. More details are provided in the forthcoming subsections.

6280



| | FRAME | ASSESS | RESPOND | MONITOR |
|---|---|---|---|---|
| **Enterprise** | • Define C-SCRM assumptions, constraints, risk appetite/ tolerance, and priorities/tradeoffs, <br> • Define C-SCRM Governance and Operating Model <br> • Develop C-SCRM Strategy, Policies, and High-Level Implementation Plan <br> • Integrate C-SCRM into enterprise risk management | • Refine/enhance organization's C-SCRM Frame <br> • Assess organization-level cyber supply chain risks based on Frame assumptions and/or analyses completed at Level 2 <br> • Determine cyber supply chain risk exposure of the organization's operations, assets, and individuals | • Make organization decisions to accept, avoid, mitigate, share, and/or transfer risk <br> • Select, tailor, and implement C-SCRM controls, including common control baselines <br> • Document C-SCRM controls in POA&Ms | • Integrate C-SCRM into the organization's Continuous Monitoring program <br> • Monitor and evaluate organization-level assumptions, constraints, risk appetite / tolerance, priorities/tradeoffs and identified risks <br> • Monitor effectiveness of organization-level risk response |
| **Mission/Business Process** | • Tailor organization C-SCRM assumptions, constraints, risk appetite/tolerance, priorities/tradeoffs to the mission/business <br> • Develop mission/business specific C-SCRM strategies, policies, and implementation plans <br> • Integrate C-SCRM into mission/business processes | • Refine/enhance criticality assumptions about the mission/business-specific operations, assets, and individuals <br> • Assess mission/business specific threats, vulnerabilities, likelihoods, and impacts <br> • Determine cyber supply chain risk exposure of mission /business-specific operations, assets, and individuals | • Make mission/business-level decisions to accept, avoid, mitigate, share, or transfer risk <br> • Select, tailor, & implement appropriate mission/ business-level controls, including common control baselines <br> • Document C-SCRM controls in POA&Ms | • Integrate C-SCRM into Continuous Monitoring processes and systems <br> • Monitor and evaluate mission-level assumptions, constraints, risk appetite / tolerance, priorities/tradeoffs and identified risks <br> • Monitor effectiveness of mission-level risk response |
| **Operational** | • Apply/tailor C-SCRM Framing from Levels 1 and 2 to individual systems in accordance with the RMF outlined in NIST 800-37, Revision 2 <br> • Integrate C-SCRM throughout the SDLC | • Assess Operational-specific cyber supply chain risks arising from components or services provided through the supply chain in accordance with the RMF outlined in NIST 800-37, Revision 2 | • Adopt Operational-specific C-SCRM controls in accordance with the *Select, Implement, Assess, and Authorize* steps of NIST SP 809-37, Revision 2 | • Monitor the system and Operational-level C-SCRM controls in accordance with the *Monitor* step of RMF outlined in NIST SP 809-37, Revision 2 |

6281

6282 **Fig. C-2: C-SCRM Activities in The Risk Management Process[22]**

6283

6284 Figure C-2 depicts interrelationships among the risk management process steps including the
6285 order in which each analysis is executed, and the interactions required to ensure the analysis is
6286 inclusive of the various inputs at the organization, mission, and operations levels.

6287

6288 The remainder of this section provides a detailed description of C-SCRM activities within the
6289 Frame, Assess, Respond, and Monitor steps of the Risk Management Process. The structure of
6290 subsections *Frame* through *Monitor* mirrors the structure of NIST SP 800-39, Sections 3.1-3.4.
6291 For each step of the Risk Management Process (i.e., Frame, Assess, Respond, Monitor), the
6292 structure includes Inputs and Preconditions, Activities, and Outputs and Post-Conditions.
6293 Activities are further organized into Tasks according to [NIST SP 800-39]. NIST SP 800-161
6294 cites the steps and tasks of the risk management process but rather than repeating any other
6295 content of [NIST SP 800-39], it provides C-SCRM-specific guidance for each step with its
6296 Inputs and Preconditions, Activities with corresponding Tasks, and Outputs and Post-Conditions.
6297 NIST SP 800-161 adds one task to the tasks provided in [NIST SP 800-39], under the Assess
6298 step: Task 2-0, *Criticality Analysis*.

6299

---

[22] More detailed information on the Risk Management Process can be found in Appendix C

**Target Audience**

The target audience for this appendix is those individuals with specific C-SCRM responsibilities for performing the supply chain risk management process across and at each level. Examples include those process/functional staff responsible for defining the frameworks and methodologies used by the rest of the organization (e.g., C-SCRM PMO Processes, Enterprise Risk Management, Mission/Business Process Risk Managers, etc.). Other personnel or entities are free to make use of the guidance as appropriate to their situation.

**Organization-wide Risk Management & the RMF**

Managing cyber supply chain risk requires a concerted and purposeful effort by organizations across organization, mission/business process, and operational-levels. This document describes two different but complementary risk management approaches which are iteratively combined to facilitate effective risk management across the 3 levels.

The first approach known as FARM consists of 4 steps: Frame, Assess, Respond, Monitor. FARM is primarily used at Levels 1 and 2 to establish the organization's risk context and inherent exposure to risk. Then, the risk context from Levels 1 and 2 iteratively informs activities performed as part of the second approach described in [NIST SP 800-37r2] The Risk Management Framework (RMF). The RMF predominantly operates at Level 3[23] – the operational level, and consists of 7 process steps: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor[z]. Within the RMF, inputs from FARM at Levels 1 and 2 are synthesized as part of the RMF Prepare step, then iteratively applied, tailored and updated through each successive step of the RMF. Ultimately Level 1 and 2 assumptions are iteratively customized and tailored to fit the specific operational-level or procurement-action context. For example, an organization may decide on strategic priorities and threats at Level 1 (enterprise level), which inform the criticality determination of missions/business processes at Level 2, which in turn influence the system categorization, control selection, and control implementation as part of the RMF at Level 3 (operational-level). Information flow between the levels is bidirectional with aggregated Level 3 RMF outputs serving to update and refine assumptions made at Levels 1 and 2 on a periodic basis.

**FRAME**
**Inputs and Preconditions**

*Frame* is the step that establishes context for C-SCRM in all three levels. The scope and structure of the organizational cyber supply chain, the overall risk management strategy, specific program/project strategies and plans, and individual information systems are defined in this step. The data and information collected during Frame provides inputs for scoping and fine-tuning C-SCRM activities in other risk management process steps throughout the three levels. Frame is also where guidance in the form of frameworks and methodologies is established as part of the organization and mission/business process level risk management strategies. These frameworks

---
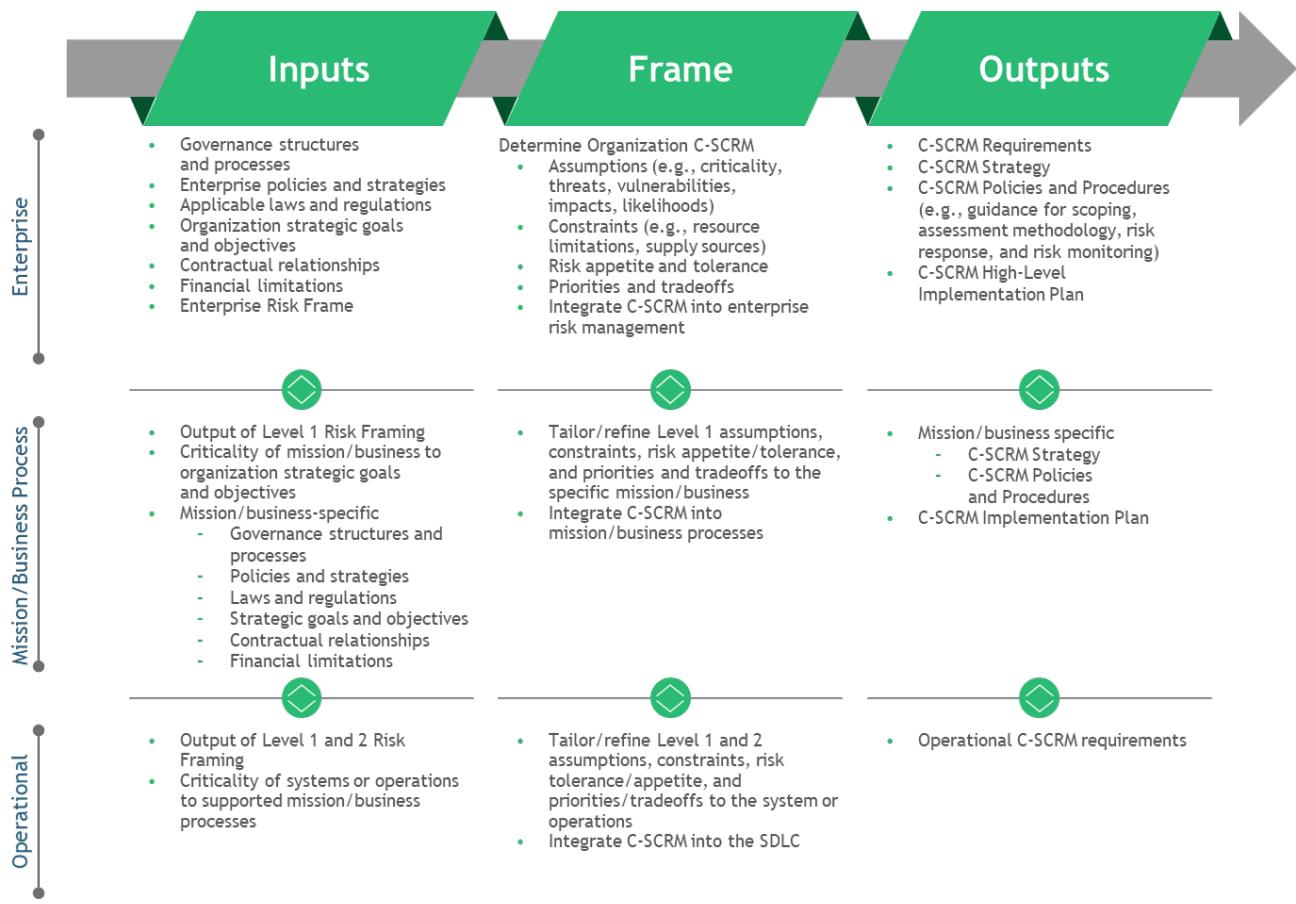
[23] The RMF does have some applications at Levels 1 and 2 such as the identification of common controls.

6342    and methodologies provide bounds, standardization, and orientation for cyber supply chain risk
6343    management activities performed within later steps.
6344
6345    [NIST SP 800-39] defines risk framing as "the set of assumptions, constraints, risk tolerances,
6346    and priorities/trade-offs that shape an organization's approach for managing risk." Organization-
6347    wide and C-SCRM risk framing activities should iteratively inform one another. Assumptions
6348    the organization makes about risk should flow down and inform risk framing within C-SCRM
6349    activities (e.g., organization's strategic priorities). As the organization's assumptions about cyber
6350    supply chain risk evolve through the execution of C-SCRM activities, these assumptions should
6351    flow up and inform how risk is framed at the enterprise level (e.g., level of risk exposure to
6352    individual suppliers). Inputs into the C-SCRM risk framing process include, but are not limited
6353    to:
6354
6355        • Organization policies, strategies, and governance
6356        • Applicable laws and regulations
6357        • Agency critical suppliers and contractual services
6358        • Organization processes (security, quality, etc.)
6359        • Organization threats, vulnerabilities, risks, and risk tolerance
6360        • Enterprise architecture
6361        • Mission-level goals and objectives
6362        • Criticality of missions/processes
6363        • Mission-level security policies
6364        • Functional requirements
6365        • Criticality of supplied system/product components
6366        • Security requirements
6367
6368    C-SCRM risk framing is an iterative process that also uses inputs from the other steps of the risk
6369    management processes (Assess, Respond, and Monitor) as inputs. Figure 2-5 depicts the Frame
6370    Step with its inputs and outputs along the three organizational levels. At the enterprise level, the
6371    organization will be concerned with conditions (i.e., assumptions, constraints, appetites and
6372    tolerances, and priorities and tradeoffs) that are broadly applicable across the organization and
6373    focus on contextualizing cyber supply chain risk to the organization's strategic goals and
6374    objectives. At the mission/business process level, frame activities focus on the individual mission
6375    and business process segments (e.g., assumptions about a technology assets or service provider's
6376    role in enabling enterprise-level objectives to be met). Level 2 frame activities take cyber supply
6377    chain risk conditions framed at Level 1, and tailor and contextualize them to reflect the role
6378    cyber supply chain risk has in each individual mission/business process to meet operational
6379    objectives. Finally, at Level 3, conditions outlined at Levels 1 and 2 iteratively inform each step
6380    of the RMF process. Beginning with the Prepare step, conditions outlined at Levels 1 and 2 are
6381    used to establish the context and priorities for managing cyber supply chain risk with respect to
6382    individual information systems, supplied system components, and system services providers.
6383    Then with each subsequent RMF step (Categorize through Monitor), these assumptions are
6384    iteratively updated and tailored to reflect applicable operational-level considerations. Information
6385    flow must be bi-directional between levels as insights discovered while performing lower level
6386    activities may update what is known about conditions outlined in higher levels.

6387
6388



6389
6390                        **Fig. C-3: C-SCRM in the Frame Step[24]**

6391
6392
6393    Figures C-3 – C-6 depict inputs, activities, and outputs of the Frame Step distributed along the
6394    three risk management framework levels. The large arrows on the left and right sides of the
6395    activities depict the inputs and outputs to and from other steps of the Risk Management Process,
6396    with the arrow on the left depicting that steps are in constant interaction. Inputs into the Frame
6397    Step include inputs from other steps as well as inputs from the organization risk management
6398    process that are shaping the C-SCRM process. Up-down arrows between the levels depict flow
6399    of information and guidance from the upper levels to the lower levels and the flow of
6400    information and feedback from the lower levels to the upper levels. Together the arrows indicate
6401    that the inputs, activities, and outputs are continuously interacting and influencing one another.
6402
6403    As the Frame step is used to define the cyber supply chain risk conditions, organizations may
6404    find that Frame activities are performed relatively less often than the latter steps of the FARM
6405    process. Organizations may re-perform Frame activities at defined intervals (e.g., annually, bi-

---

[24] More detailed information on the Risk Management Process can be found in Appendix

6406   annually) or based on defined triggers (e.g., based on business changes and/or new or updated
6407   insights from other levels).
6408
6409   **Activities**
6410   RISK ASSUMPTIONS

6411   **TASK 1-1:** Identify assumptions that affect how risk is assessed, responded to, and monitored
6412   within the organization.
6413
6414   **Supplemental Guidance**
6415
6416   As a part of identifying cyber supply chain risk assumptions within the broader Risk
6417   Management process (described in [NIST SP 800-39]), agencies should do the following:
6418
6419      •   Develop an organization-wide C-SCRM policy;
6420      •   Identify which mission and business processes and related components are critical to the
6421          organization to determine the **criticality**;
6422      •   Define which mission and business processes and information systems compose the
6423          cyber supply chain, including relevant contracted services and commercial products;
6424      •   Prioritize the application of risk treatment for these critical elements, considering factors
6425          such as but not limited to national and homeland security concerns, FIPS 199 impact
6426          level, scope of use, or interconnections/interdependencies to other critical processes and
6427          assets;
6428      •   Identify, characterize, and provide representative examples of **threat sources**,
6429          **vulnerabilities**, **consequences/impacts**, and **likelihood** determinations related to cyber
6430          supply chain;
6431      •   Define C-SCRM mission, business, and operational-level requirements;
6432      •   Select appropriate cyber supply chain risk assessment methodologies, depending on
6433          organizational governance, culture, and diversity of the mission and business processes;
6434      •   Establish a method for the results of C-SCRM activities to be integrated into the overall
6435          agency Risk Management Process;
6436      •   Periodically review the cyber supply chain to ensure definition remains current as
6437          evolutions occur over time.
6438
6439   These supply chain risk assumptions should be aligned as applicable to the organization's
6440   broader set of risk assumptions defined as part of the enterprise risk management program. A key
6441   C-SCRM responsibility (e.g., of the C-SCRM PMO) is identifying which of those assumptions
6442   apply to the cyber supply chain risk context at each successive risk management framework
6443   level.  If and when new C-SCRM assumptions are identified, these should be provided as
6444   updates to the enterprise risk assumptions as part of an iterative process.
6445
6446   *Criticality*
6447
6448   Critical processes are those processes, which if disrupted, corrupted or disabled, are likely to
6449   result in mission degradation or failure. Mission-critical processes are dependent on their
6450   supporting systems that in turn depend on critical components in those systems (hardware,

6451    software, and firmware). Mission-critical processes also depend on information and processes
6452    (performed by technology or people, to include in some instances, support service contractors),
6453    that are used to execute the critical processes. Those components and processes that underpin
6454    and enable mission-critical processes or deliver defensive—and often commonly shared—
6455    processes (e.g., access control, identity management, and crypto) and unmediated access (e.g.,
6456    power supply) should also be considered critical. A criticality analysis is the primary method by
6457    which mission-critical processes, associated systems/components, and enabling infrastructure
6458    and support services are identified and prioritized. The criticality analysis also involves
6459    analyzing critical suppliers which may not be captured by internal criticality analysis (e.g.,
6460    supply chain interdependencies including 4th and 5th party suppliers)
6461
6462    Organizations will make criticality determinations as part of enterprise risk management
6463    activities based on the process outlined in [NISTIR 8179].[25] Where possible, C-SCRM should
6464    inherit those assumptions and tailor/refine them to include the C-SCRM context. In C-SCRM,
6465    criticality tailoring includes initial criticality analysis of particular projects, products, and
6466    processes in the supply chain in relation to critical processes at each Level. For example, at Level
6467    1 the enterprise may determine the criticality of holistic supplier relationships to the
6468    organization's overall strategic objectives. Then at Level 2, the organization may assess the
6469    criticality of individual suppliers, products and services to specific mission/business processes
6470    and strategic/operational objectives. Finally, at Level 3, the organization may assess the
6471    criticality of the supplied product or service to specific operational state objectives of the
6472    information systems.
6473
6474    Organizations may begin by identifying key supplier-provided products or services which
6475    contribute to the operation and resiliency of organizational processes and systems. The criticality
6476    determination may be based on the role of each supplier, product, or service in achieving the
6477    required strategic or operational objective of the process or system. Requirements, architecture,
6478    and design inform the analysis and help identify the minimum set of supplier-provided products
6479    and/or services required for operations (i.e., at organization, mission/business process, and
6480    operational-levels). The analysis combines top-down and bottom-up analysis approaches. The
6481    top-down approach in this model enables the organization to identify critical processes and then
6482    progressively narrow the analysis to critical systems that support those processes, and finally to
6483    critical components which support the critical functions of those systems.  The bottom-up
6484    approach progressively traces the impact of a malfunctioning, compromised, or unavailable
6485    critical component would have on the system, and in turn, on the related mission and business
6486    process.
6487
6488    Organizations performing this analysis should include agency system and cyber supply chain
6489    dependencies, to include critical 4th-party suppliers. For example, an organization may find
6490    cyber supply chain risk exposures that result from 3rd-party suppliers receiving critical input or
6491    services from a common 4th-party supplier.
6492
6493    Determining criticality is an iterative process performed at all levels during both Frame and
6494    Assess. In Frame, criticality determination is expected to be performed at a high level, using the

---

[25] NISTIR 8179: Criticality Analysis Process Model: Prioritizing Systems and Components

6495    available information with further detail incorporated through additional iterations or at the
6496    Assess step. Determining criticality may include, but is not limited to, the following:
6497
6498        •   Define criticality analysis procedures to ensure there is a set of documented procedures to
6499            guide the organization's criticality analysis across levels;
6500        •   Conduct organization and mission-level criticality analysis to identify and prioritize
6501            organization and mission objectives, goals and requirements;
6502        •   Conduct operational-level criticality analysis (i.e., systems and subsystems) to identify
6503            and prioritize critical workflow paths, system functionalities and capabilities;
6504        •   Conduct system and subsystem component-level criticality analysis to identify and
6505            prioritize key system and subsystem inputs (e.g., COTS products);
6506        •   Conduct detailed review (e.g., bottom-up analysis) of impacts and interactions between
6507            organization, mission, system/sub systems, and components/subcomponents to ensure
6508            cross-process interaction and collaboration.
6509
6510    Please note that criticality can be determined for existing systems or for future system
6511    investments, development, or integration efforts based on system architecture and design. It is an
6512    iterative activity that should be performed when a change warranting iteration is identified in the
6513    Monitor step.
6514
6515    *Threat Sources*
6516
6517    For C-SCRM, threat sources include: (i) adversarial threats such as cyber/physical attacks either
6518    to the supply chain or to an information system component(s) traversing the supply chain; (ii)
6519    accidental human errors; (iii) structural failures which include failure of equipment,
6520    environmental controls, resource depletion; and (iv) environmental threats such as geopolitical
6521    disruptions, pandemics, economic upheavals, and natural or man-made disasters. With regard to
6522    adversarial threats, [NIST SP 800-39] states that organizations provide a succinct
6523    characterization of the types of tactics, techniques, and procedures employed by adversaries that
6524    are to be addressed by safeguards and countermeasures (i.e., security controls) deployed at Level
6525    1 (enterprise-level), at Level 2 (mission/business process level), and at Level 3 (information
6526    system/services level)—making explicit the types of threat sources to be addressed as well as
6527    making explicit the threat sources not being addressed by the safeguards/countermeasures.
6528
6529    Threat information can include but is not limited to historical threat data, factual threat data, or
6530    business entity (e.g., suppliers, developers, system integrators, external system service providers,
6531    and other ICT/OT-related service providers) or technology-specific threat information. Threat
6532    information may come from multiple information sources, including the U.S. Intelligence
6533    Community (for federal agencies), DHS, CISA, the FBI, as well as open-source reporting such as
6534    news and trade publications, partners, suppliers, and customers. When applicable, organizations
6535    may rely on the Federal Acquisition Security Council's (FASC) Information Sharing Agency
6536    (ISA) for supply chain threat information in addition the aforementioned sources. As threat
6537    information may include classified intelligence, it is crucial that departments and agencies have
6538    the capabilities required to process classified intelligence. Threat information obtained as part of
6539    the Frame step should be used to document the organization's long-term assumptions about
6540    threat conditions based on its unique internal and external characteristics. During the Assess step,

6541   updated information is infused into the risk assessment to account for short-term variations in
6542   threat conditions (e.g., due to geopolitical circumstances) as well as to obtain supply chain threat
6543   information that is specifically relevant and essential to inform the risk-based analysis and
6544   decision-making concerning the procurement of a given product or a service.
6545
6546   Information about cyber supply chain (such as supply chain maps) provides the context for
6547   identifying possible locations or access points for threat sources and agents to affect the cyber
6548   supply chain. The cyber supply chain threats are similar to the information security threats, such
6549   as disasters, attackers, or industrial spies. Table C-1 lists examples of cyber supply chain threat
6550   agents. Appendix D provides Risk Response Plans that provide examples of the Supply Chain
6551   Threat Sources and Threats listed in Table C-1.
6552
6553

**Table C-1: Examples of Cyber Supply Chain Threat Sources/Agents**

| Threat Sources | Threat | Examples |
|---|---|---|
| Adversarial:<br><br>Counterfeiters | Counterfeits inserted into cyber supply chain (see Appendix B Scenario 1) | Criminal groups seek to acquire and sell counterfeit cyber components for monetary gain. Specifically, organized crime groups seek disposed units, purchase overstock items, and acquire blueprints to obtain cyber components intended for sale through various gray market resellers to acquirers.[26] |
| Adversarial:<br><br>Malicious Insiders | Intellectual property loss | Disgruntled insiders sell or transfer intellectual property to competitors or foreign intelligence agencies for a variety of reasons including monetary gain. Intellectual property includes software code, blueprints, or documentation. |
| Adversarial:<br><br>Foreign Intelligence Services | Malicious code insertion (see Appendix B Scenario 3) | Foreign intelligence services seek to penetrate cyber supply chain and implant unwanted functionality (by inserting new or modifying existing functionality) into system to gather information or subverting[27] system or mission operations when system is operational. |

---

[26] "Defense Industrial Base Assessment: Counterfeit Electronics," [*Defense Industrial Base Assessment: Counterfeit Electronics*].

[27] Examples of subverting operations include gaining unauthorized control to cyber supply chain or flooding it with unauthorized service requests to reduce or deny legitimate access to cyber supply chain.

[5]Information and Communications Technology Supply Chain Risk Management Task Force: Threat Evaluation Working. Group: Threat Scenarios Version 2.0

| Adversarial: Terrorists | Unauthorized access | Terrorists seek to penetrate or disrupt the cyber supply chain and may implant unwanted functionality to obtain information or cause physical disablement and destruction of systems through the cyber supply chain. |
|---|---|---|
| Adversarial: Industrial Espionage/Cyber Criminals | Industrial Espionage/Intellectual Property Loss (see Appendix B Scenario 2) | Industrial spies/cyber criminals seek ways to penetrate cyber supply chain to gather information or subvert system or mission operations (e.g., exploitation of an HVAC contractor to steal credit card information). |
| Systemic: Legal/Regulatory | Legal/regulatory complications impact the availability of key supplier-provided products and/or services | Weak anti-corruption laws, lack of regulatory oversight, weak intellectual property considerations: this also includes the threats resulting from country-specific laws, policies, and practices intended to undermine competition and free market protections such as the requirement to transfer technology and intellectual property to domestic providers in a foreign country.[5] |
| Systemic Economic Risks | Business failure of a key supplier leads to supply chain disruption | Economic risks stem from threats to the financial viability of suppliers and the potential impact to the supply chain resulting from the failure of a key supplier as a result. Other threats to the supply chain that result in economic risks include, but are not limited to, vulnerabilities to cost volatility, reliance on single source suppliers, cost to swap out suspect vendors, and resource constraints due to company size.[5] |
| Environmental: Disasters | Geopolitical or natural disaster lead to supply chain disruption | Availability of key supply chain inputs is subject to disruptions from geopolitical upheavals or natural disasters. This is especially the case when suppliers share a common 4th-party supplier, |

| Structural: Hardware Failure | Inadequate capacity planning leads to outage in cloud platform | A vendor or supplier service without the appropriate capacity controls in place could be subject to disruptions in the event of unexpected surges in resource demand. |
| --- | --- | --- |
| Accidental: Negligent Insiders | Configuration error leads to data exposure | Employees and contractors with access to information systems are prone to errors which could result in the disclosure of sensitive data. This is specifically true in cases where training lapses or process gaps increase the opportunities for errors. |

6554

6555 Agencies can identify and refine C-SCRM-specific threats in all three levels. Table C-2
6556 provides examples of threat considerations and different methods for use in characterizing cyber
6557 supply chain threats at different levels.

6558
6559 **Table C-2: Supply Chain Threat Considerations**

| Level | Threat Consideration | Methods |
| --- | --- | --- |
| Level 1 | • Organization business and mission<br>• Strategic supplier relationships<br>• Geographical considerations related to the extent of the organization's cyber supply chain | • Establish common starting points for identifying cyber supply chain threat.<br>• Establish procedures for countering organization-wide threats such as insertion of counterfeits into critical systems and components. |
| Level 2 | • Mission and business processes<br>• Geographic locations<br>• Types of suppliers (COTS, external service providers, or custom, etc.)<br>• Technologies used organization-wide | • Identify additional sources of threat information specific to organizational mission and business processes.<br>• Identify potential threat sources based on the locations and suppliers identified through examining available agency cyber supply chain information (e.g., from supply chain map).<br>• Scope identified threat sources to the specific mission and business processes, using the agency the cyber supply chain information.<br>• Establish mission-specific preparatory procedures for countering threat adversaries/natural disasters. |

| Level 3 | • SDLC | • Base the level of detail with which threats should be considered on the SDLC phase.<br>• Identify and refine threat sources based on the potential for threat insertion within individual SDLC processes. |
|---|---|---|

6560

6561 *Vulnerabilities*

6562

6563 A vulnerability is a weakness in an information system, system security procedures, internal
6564 controls, or implementation that could be exploited or triggered by a threat source [FIPS 200],
6565 [NIST SP 800-34 Rev. 1], [NIST SP 800-53 Rev 4], [NIST SP 800-53A Rev. 4], [NIST SP 800-
6566 115]. Within the C-SCRM context, it is any weakness in the supply chain, provided services,
6567 system/component design, development, manufacturing, production, shipping and receiving,
6568 delivery, operation, and component end-of-life that can be exploited by a threat source. This
6569 definition applies to both the services/systems/components being developed and integrated (i.e.,
6570 within the SDLC) and to the cyber supply chain, including any security mitigations and
6571 techniques, such as identity management or access control systems. Vulnerability assumptions
6572 made in the Frame step of the FARM process capture the organization's long-term assumptions
6573 about the organization's weaknesses that can be exploited or triggered by a threat source. These
6574 will become further refined and updated to reflect point-in-time variances during the Assess step.
6575 Organizations may make long-term cyber supply chain vulnerability assumptions about:

6576

6577 • The entities within supply chain itself (e.g., individual supplier relationships);
6578 • The critical services provided through the supply chain which support the organization's
6579   critical missions and business processes;
6580 • The products/systems/components provided through the supply chain and used within the
6581   SDLC (i.e., being developed and integrated);
6582 • The development and operational environment directly impacting the SDLC; and
6583 • The logistics/delivery environment that transports systems and components (logically or
6584   physically).

6585

6586 Vulnerabilities manifest differently across the 3 levels (i.e., organization, mission/business
6587 process, information system). At Level 1, vulnerabilities present as susceptibilities of the
6588 organization at-large due to managerial and operating structures (e.g., policies, governance,
6589 processes) as well as conditions in the supply chain (e.g., concentration of products or services
6590 from a single supplier) or critical enterprise processes (e.g., use of a common system across
6591 critical processes). At Level 2, vulnerabilities are specific to a mission/business process and
6592 result from its operating structures and conditions such as reliance on a specific system or
6593 supplier provided input, or service to achieve specific mission/business process operating
6594 objectives. Level 2 vulnerabilities may vary widely across the different mission/business
6595 processes. Within Level 3, vulnerabilities manifest as supplied product or operational-level
6596 weaknesses or deficiencies arising from the SDLC, system security procedures, internal controls,

6597　implementations, as well as system inputs or services provided through the supply chain (e.g.,
6598　system components, services).
6599
6600　Organizations should identify approaches to characterize cyber supply chain vulnerabilities
6601　consistent with the characterization of threat sources and events and with the overall approach
6602　employed by the organization for characterizing vulnerabilities. Vulnerabilities may be relevant
6603　to a single threat source or broadly applicable across threat sources (adversarial, structural,
6604　environmental, accidental). For example, a single point of failure in a network may be subject to
6605　disruptions caused by environmental threats (e.g., disasters) as well as adversarial threats
6606　(terrorists). Appendix B provides examples of cyber supply chain threats, based on [NIST SP
6607　800-30 Rev. 1, Appendix B].
6608
6609　All three levels should contribute to determining the organization's approach to characterizing
6610　vulnerabilities, with progressively more detail identified and documented in the lower levels.
6611　Table C-3 provides examples of considerations and different methods for use in characterizing
6612　cyber supply chain vulnerabilities at different levels.
6613

6614　　　　　　　　　**Table C-3: Cyber Supply Chain Vulnerability Considerations**

| Level | Vulnerability Consideration | Methods |
|---|---|---|
| Level 1 | • Enterprise mission/business<br>• Holistic supplier relationships (e.g., system integrators, COTS, external services)<br>• Geographical considerations related to the extent of the organization's cyber supply chain<br>• Enterprise/Security Architecture<br>• Criticality | • Examine agency cyber supply chain information including that from supply chain maps to identify especially vulnerable entities, locations, or organizations.<br>• Analyze agency mission for susceptibility to potential supply chain vulnerabilities.<br>• Examine 3rd party provider/ supplier relationships and interdependencies for susceptibility to potential supply chain vulnerabilities.<br>• Review enterprise architecture and criticality to identify areas of weakness requiring more robust cyber supply chain considerations. |
| Level 2 | • Mission and business processes<br>• Geographic locations<br>• Mission/process level supplier dependencies (e.g., outsourced or contracted services)<br>• Technologies used | • Refine analysis from Level 1 based on specific mission and business processes and applicable threat and supply chain information.<br>• If appropriate, use the National Vulnerability Database (NVD), including Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS), to characterize, categorize, and |

| | | |
|---|---|---|
| | | score vulnerabilities[28] or other acceptable methodologies.<br>• Consider using scoring guidance to prioritize vulnerabilities for remediation. |
| Level 3 | • Individual technologies, solutions, and services should be considered<br>• Supply chain SDLC inputs such as system components or services | • Refine analysis based on inputs from related Level 2 missions and business processes.<br>• Use CVEs where available to characterize and categorize vulnerabilities.<br>• Identify weaknesses. |

6615

6616　*Consequences and Impact*

6617

6618　Impact is the effect on organizational operations, organizational assets, individuals, other
6619　organizations, or the Nation (including the national security interests of the United States) of a
6620　loss of confidentiality, integrity, or availability of information or an information system [NIST
6621　SP 800-53 Rev.5]. Impact estimated within the Frame step represents the organization's long-
6622　term assumptions about the effects different cyber events will have on its primary processes.
6623　These assumptions are updated and refined as part of the Assess step to ensure that point-in-time
6624　relevant information (e.g., market conditions)—which may alter the impact scope, duration, or
6625　magnitude—is appropriately reflected in the analysis.

6626

6627　When possible, organizations should inherit assumptions made by the organization on
6628　consequences and impact as part of enterprise risk management activities. For example, one of
6629　these activities is performing an impact analysis (BIA) on a periodic business to determine or
6630　revalidate mission-critical and mission-enabling processes, as part of the organization's
6631　continuity and emergency preparedness responsibilities. However, these assumptions may need
6632　to be developed if they do not yet exist. Organizations may maintain impact or loss libraries
6633　which capture the organization's standing assumptions about the impact of different cyber event
6634　types (e.g., disclosure, disruption, destruction, modification) on the organization's assets. These
6635　libraries may break down impact and loss into individual impact types (e.g., operational,
6636　reputational, regulatory/legal fines and penalties, IT recovery/replacement, direct financial,
6637　damage to critical infrastructure sector).

6638

6639　For C-SCRM, organizations should refine and update their consequences and impact
6640　assumptions to reflect the role that availability, confidentiality and integrity of supplier-provided
6641　products or services have on the organizational operations, assets, and individuals. For example,
6642　depending on its criticality, the loss of a key supplier-provided input or service may reduce the
6643　organization's operational capacity or completely inhibit its operations. In this publication,

---

[28] See https://nvd.nist.gov/

6644    impact is always in relation to the organization's mission and includes the systems or
6645    components traversing the supply chain as well as the supply chain itself.
6646
6647    C-SCRM consequences and impact will manifest differently across all three levels in the risk
6648    management hierarchy. Impact determinations require a combined top-down and bottom-up
6649    approach. Table C-4 provides examples of how consequences and impact may be characterized
6650    at different levels of the organization:
6651

6652                    **Table C-4: Cyber Supply Chain Consequence & Impact Considerations**

| Level | Impact Considerations | Methods |
|---|---|---|
| Level 1 | <ul><li>General enterprise-level impact assumptions</li><li>Supplier criticality (e.g., holistic supplier relationships)</li></ul> | <ul><li>Examine magnitude of exposure to individual entities within the supply chain.</li><li>Refine Level 2 analysis to determine aggregate Level 1 impact on the organization's primary function resulting from cyber events to and through the supply chain.</li></ul> |
| Level 2 | <ul><li>Process role in organization's primary function</li><li>Supplier criticality to mission/process (inputs and services)</li></ul> | For each type of cyber event:<ul><li>Refine Level 3 analysis to determine aggregate mission/business process impact due to operational-level impacts from cyber events to and through the supply chain.</li><li>Examine supplier network to identify business/mission-level impacts due to events affecting individual supplier entities.</li></ul> |
| Level 3 | <ul><li>Criticality of upstream and downstream Level 2 processes</li><li>System criticality</li><li>Supplier criticality to system operations (system components and services)</li></ul> | <ul><li>Examine the systems aggregated criticality to Level 1 and Level 2 primary processes</li><li>Examine the criticality of supplied system components or services to the system's overall function.</li><li>Examine supplier network to identify individual entities which may disrupt availability of critical system inputs or services.</li></ul> |

6653

6654    Organizations should look to several sources for information that helps contextualize
6655    consequences and impact. Historical data is preferential and can be gathered by reviewing
6656    historical data for the agency, similar peer organizations, supplier organizations, or applicable
6657    industry surveys. Where gaps in historical data exist, organizations should consider the use of
6658    expert elicitation protocols (e.g., calibrated estimation training) which make use of the tacit
6659    knowledge of appropriate individuals across the organization. By interviewing well positioned
6660    experts (e.g., technology or mission/business owners of assets) organizations can tailor impact
6661    assumptions to reflect the organization's unique conditions and dependencies. NISTIR 8286

6662    offers a more in-depth discussion of how different quantitative and qualitative methodologies can
6663    be used to analyze risk.
6664
6665    The following are examples of cyber supply chain consequences and impact:
6666       • An earthquake in Malaysia reduces the amount of commodity Dynamic Random-Access
6667         Memory (DRAM) to 60 percent of the world's supply, creating a shortage for hardware
6668         maintenance and new design;
6669       • Accidental procurement of a counterfeit part results in premature component failure,
6670         thereby impacting the organization's mission performance;
6671       • Disruption in at a key cloud service provider resulting in operational downtime losses
6672         between $1.5M – $15M dollars.
6673
6674    *Likelihood*
6675
6676    In an information security risk analysis, likelihood is a weighted factor based on a subjective
6677    analysis of the probability that a given threat is capable of exploiting a given vulnerability
6678    [CNSSI 4009]. General likelihood assumptions should be inherited from the organization's
6679    enterprise risk management process then refined to account for C-SCRM specific implications
6680    however, the general assumptions may need developing if they do not yet exist. Likelihood
6681    analysis in the Frame step sets the organization's long-term assumptions about the relative
6682    likelihood of different adverse cyber events. Likelihood is subject to extreme short-term
6683    variations based on point-in-time conditions (i.e., internal and external) and thus must be updated
6684    and refined as part of the Assess step.
6685
6686    In adversarial cases a likelihood determination may be made using intelligence trend data,
6687    historical data, and expert intuition on (i) adversary intent; (ii) adversary capability; and (iii)
6688    adversary targeting. In non-adversarial cases (e.g., structural, environmental, accidental),
6689    likelihood determinations will draw on expert intuition and historical data. When available,
6690    historical data may help further reduce uncertainty about what cyber supply chain risks are
6691    probable to occur. Historical data may be sourced from internal sources (e.g., frequency of past
6692    security incidents, threat intelligence on threat activity levels) as well as external sources (e.g.,
6693    peer org. data, info-sharing). Likelihood analysis can leverage many of the same expert
6694    elicitation protocols as consequences and impact. Similar to consequences and impact, likelihood
6695    determinations may rely on qualitative or quantitative form and draw on similar techniques. To
6696    ensure likelihood is appropriately contextualized for decision makers, organizations should make
6697    time-bound likelihood estimates for cyber events affecting the supply chain (e.g., likelihood
6698    within a given year).
6699
6700    Likelihood analysis will manifest differently across the three levels. Table C-5 captures some of
6701    the considerations and methods specific to each level:
6702

6703                  **Table C-5: Cyber Supply Chain Likelihood Considerations**

| Level | Likelihood Consideration | Methods |
|---|---|---|
| Level 1 | • General threat and likelihood assumptions for the organization<br>• Level 2 and 3 likelihood findings<br>• Overall engagement models with suppliers that alter opportunities for contact with threat sources | • Analyze critical national infrastructure implications which may increase the organization's target value.<br>• Refine analyses from Levels 2 and 3 to determine aggregate exposure to threat source contact. |
| Level 2 | • Mission/process level threat and likelihood assumptions<br>• Mission/process level engagement model with suppliers (e.g., criticality of assets interacted with)<br>• Level 3 findings for relevant systems | • Evaluate mission/business process level conditions which present opportunities for threat sources to come into contact with processes or assets via the supply chain.<br>• Evaluate the aggregate supply chain threat conditions facing key systems relied upon by the mission/business process. |
| Level 3 | • Organization system threat and likelihood assumptions<br>• Supplier & system target value<br>• Location & operating conditions<br>• Supplier & system security policies, processes, and controls<br>• Nature and degree of supplier contact with system (inputs, services) | • Analyze nature of system inputs coming through the supply chain into the SDLC which alter likelihood of encountering threat sources.<br>• Evaluate the systems role in Level 1 and Level 2 processes which alter target value for potential adversaries.<br>• Analyze supply chain characteristics (e.g., location of supplier) which may increase the likelihood that a system is affected by a threat source. |

6704

6705    Agencies should determine which approach(es) they will use to determine the likelihood of a
6706    cyber supply chain compromise, consistent with the overall approach used by the agency's risk
6707    management process.  Agencies should ensure that appropriate procedures are in place to
6708    thoroughly document any risk analysis assumptions leading to the tabulation of the final risk
6709    score, especially in cases where high or critical impact risks are involved. Visibility into
6710    assumptions may be critical in enabling decision makers to take action.
6711

6712 RISK MANAGEMENT PROCESS CONSTRAINTS
6713 **TASK 1-2:** Identify constraints[29] on the conduct of risk assessment, risk response, and risk
6714 monitoring activities within the organization.
6715
6716 **Supplemental Guidance**
6717
6718 Identify the following two types of constraints to ensure the cyber supply chain is integrated into
6719 the agency risk management process:
6720
6721     1.  Agency constraints; and
6722     2.  Cyber supply chain-specific constraints.
6723
6724 Agency constraints serve as an overall input to framing the cyber supply chain policy at Level 1,
6725 mission requirements at Level 2, and system-specific requirements at Level 3. Table 2-5 lists the
6726 specific agency and cyber supply chain constraints. Cyber supply chain constraints, such as C-
6727 SCRM policy and C-SCRM requirements, may need to be developed if they do not exist.
6728
6729             **Table C-6: Cyber Supply Chain Constraints**

| Level | Agency Constraints | Cyber Supply Chain Constraints |
|---|---|---|
| Level 1 | • Enterprise policies, strategies, governance<br>• Applicable laws and regulations<br>• Mission and business processes<br>• Organization processes (security, quality, etc.)<br>• Resource limitations | • Organization C-SCRM policy based on the existing agency policies, strategies, and governance; applicable laws and regulations; mission and business processes; and organization processes.<br>• Acquisition regulations and policy.<br>• Available, mandated or restricted sources of supply or products. |
| Level 2 | • Mission and business processes<br>• Criticality of processes<br>• Enterprise architecture<br>• Mission-level security policies | • C-SCRM Mission/business requirements that are incorporated into mission/business processes and enterprise architecture.<br>• Supplier service contracts, product warranties and liability agreements. |

---

[29] Refer to [NIST SP 800-39], Section 3.1, Task 1-2 for a description of constraints in the risk management context.

| Level 3 | • Functional requirements <br> • Security requirements | • Product and Operational-level C-SCRM capabilities. <br> • Supplier-provided system component warranties and service agreements. |

6730

6731 An organization's C-SCRM policy is a critical vehicle for directing C-SCRM activities. Driven
6732 by applicable laws and regulations, this policy should support applicable organization policies
6733 including acquisition and procurement, information security, quality, and supply chain and
6734 logistics. It should address goals and objectives articulated in the overall agency strategic plan, as
6735 well as specific mission and business processes and business goals, along with the internal and
6736 external customer requirements. It should also define the integration points for C-SCRM with the
6737 agency's Risk Management Process and SDLC.
6738
6739 C-SCRM policy should define C-SCRM-related roles and responsibilities of the agency C-
6740 SCRM team, any dependencies among those roles, and the interaction among the roles. C-
6741 SCRM-related roles will articulate responsibilities for collecting cyber supply chain threat
6742 intelligence, conducting risk assessments, identifying and implementing risk-based mitigations,
6743 and performing monitoring processes. Identifying and validating roles will help to specify the
6744 amount of effort required to implement the C-SCRM Plan. Examples of C-SCRM-related roles
6745 include:
6746
6747 • C-SCRM PMO that provides overarching cyber supply chain risk guidance to
6748 engineering decisions that specify and select cyber products as the system design is
6749 finalized;
6750 • Procurement officer and maintenance engineering responsible for identifying and
6751 replacing the hardware when defective;
6752 • Delivery organization and acceptance engineers who verify that the system component is
6753 acceptable to receive into the acquiring organization;
6754 • System integrator responsible for system maintenance and upgrades, whose staff resides
6755 in the acquirer facility and uses system integrator development infrastructure and the
6756 acquirer operational infrastructure;
6757 • System Security Engineer/Systems Engineer responsible for ensuring that information
6758 system security concerns are properly identified and addressed throughout the SDLC; and
6759 • The end user of cyber systems/components/services.
6760
6761 C-SCRM requirements should be guided by C-SCRM policy(ies), as well as by the mission and
6762 business processes and their criticality at Level 2 and by known functional and security
6763 requirements at Level 3.
6764

6765 RISK APPETITE AND TOLERANCE
6766 **TASK 1-3:** Identify the levels of risk appetite and tolerance for the organization.

6767

6768  **Supplemental Guidance**

6769

6770  Risk appetite represents the types and amount of risk, on a broad level, an organization is willing
6771  to accept in pursuit of value [NISTIR 8286]. On the other hand, risk tolerance is the organization
6772  or stakeholder's readiness to bear the remaining risk after risk response in order to achieve its
6773  objectives, with the consideration that such tolerance can be influenced by legal or regulatory
6774  requirements [NISTIR 8286]. This definition is adapted from COSO, which states risk tolerance
6775  is the acceptable level of variation relative to achievement of a specific objective. Often, risk
6776  tolerance is best measured in the same units as those used to measure the related objective
6777  [COSO 2011]. Where applicable, organizations should align with risk appetite and tolerance
6778  assumptions and thresholds from the enterprise risk management process. For C-SCRM, these
6779  assumptions and thresholds should be contextualized to inform decisions in the C-SCRM
6780  domain. This may require C-SCRM define its own relevant C-SCRM-specific risk appetite and
6781  corresponding tolerance thresholds.

6782

6783  Risk appetite and tolerance strongly influence decisions made about C-SCRM across the three
6784  levels. Some organizations may define risk appetite and risk tolerance as part of their broader
6785  organization risk management activities (i.e., enterprise risk management). In organizations
6786  without a clearly defined risk appetite, Level 1 stakeholders should collaborate with organization
6787  leadership to define and articulate the organization's appetite for risk within the scope of the C-
6788  SCRM program's mandates. Organizations may choose to tailor risk appetite definitions to
6789  specific mission and business processes. In general, risk appetite at Level 1 may be set to
6790  empower the organization to meet its value objectives (e.g., high appetite for supplier risk in
6791  support of reducing operating costs by 5%). At Level 2 this may translate to relaxed C-SCRM
6792  governance structures and processes in alignment with this appetite threshold. Risk appetite
6793  definitions at lower levels should always be subject to the constraints provided at the higher
6794  levels.

6795

6796  With risk appetite defined, the organization should define its risk tolerance in order to
6797  operationalize the risk appetite across the organization. Risk tolerance should be defined for the
6798  organization as a whole as well as the specific mission and business processes. Organizations
6799  may use risk tolerance to inform cost/benefit decisions made about system components and
6800  services provided through the supply chain for systems throughout the SDLC. Risk Appetite and
6801  risk tolerance work together to guide C-SCRM decisions at various levels as the organization
6802  pursues its objectives.

6803

6804

6805  Table C-7 shows additional examples of how risk appetite and risk tolerance statements work
6806  together to frame risk within an organization.

6807

6808
**Table C-7: Risk Appetite & Risk Tolerance**

| Level | Agency Constraints | Cyber Supply Chain Constraints |
|---|---|---|
| 1 | • **Low appetite** for risk with respect to market objectives | • **Low tolerance** (i.e., no more than 5% probability) for service provider downtime that causes system disruptions to exceed contractual service level agreements (SLAs) by more than 10%. |
| 2 | • **Low appetite** for appetite for risk with respect to production objectives | • **Moderate tolerance** (i.e., no more than 15% probability) for supply chain disruptions that cause production levels to fall below 80% of target threshold for non-military products.<br><br>• **Near-zero tolerance (**i.e., no more than 5% probability) of supply chain disruptions that cause production levels to fall below 80% of target threshold for military products. |
| 3. | • **Low appetite** for risk related to national security objectives | • **Low tolerance** (i.e., no more than 1% of contractor access authorizations) for inappropriate contractor access that exceeds authorized windows by more than 10% in systems with classified information. |
| 4. | • **Low appetite** low appetite for risk related to operational objectives | • **Moderate tolerance** (i.e., no more than 15% probability) for system component failures causing non-critical system disruptions that exceed maximum allowable thresholds by more than 10%.<br><br>• **Near-zero tolerance** (i.e., no more than 3% probability) for system component failures causing disruptions in critical systems that exceed maximum allowable thresholds by more than 10%. |

6809

6810 To ensure leadership has the appropriate information when making risk-based decisions,
6811 organizations should establish metrics (e.g., Key Performance Indicators (KPIs), Key Risk
6812 Indicators (KRIs)) to measure performance against defined risk appetite and risk tolerance
6813 thresholds. Identification of corresponding data sources for measurement should play a key role
6814 in the organization's defined processes for setting and refining risk appetite and tolerance
6815 thresholds. Risk appetite and risk tolerance should be treated as dynamic thresholds by the

6816  organization. This requires periodic update and revision based on internal (e.g., strategy) and
6817  external (e.g., market, environmental) changes which impact the organization.
6818
6819  Organizations should consider cyber supply chain threats, vulnerabilities, constraints, and
6820  criticality when identifying the overall level of risk appetite and risk tolerance.[30]
6821
6822
6823  PRIORITIES AND TRADE-OFFS
6824  **TASK 1-4:** Identify priorities and trade-offs considered by the organization in managing risk.
6825
6826  **Supplemental Guidance**
6827
6828  Priorities and tradeoffs are closely linked to the organization's risk appetite and tolerance
6829  thresholds, which communicate the amount of risk that is acceptable and tolerable to the
6830  organization in pursuit of its objectives. Priorities will take the form of long-term strategic
6831  objectives or near-term strategic imperatives which alter risk decision calculus. From priorities
6832  and tradeoffs, C-SCRM then receives critical strategic context required for Response step
6833  activities such as Evaluation of Alternatives and Risk Response Decision. As a part of
6834  identifying priorities and trade-offs, organizations should consider risk appetite, risk tolerance,
6835  cyber supply chain threats, vulnerabilities, constraints, and criticality.
6836
6837  Priority and tradeoff considerations will manifest different across the 3 levels. Within Level 1,
6838  priority and tradeoff considerations may favor existing supplier relationships in established
6839  regions at the expense of new supplier cost advantages due to a desire to maintain confidence
6840  and stability. At Level 2, priority and tradeoff considerations may favor centralized C-SCRM
6841  governance models covering product teams in favor of greater security practice standardization.
6842  At Level 3, priorities and tradeoffs may favor system components/subcomponents produced in
6843  certain geographies in an effort to avoid environmental or geopolitical risks to the supply chain.
6844

6845  **Outputs and Post Conditions**
6846  Within the scope of NIST SP 800-39, the output of the risk framing step is the risk management
6847  strategy that identifies how organizations intend to assess, respond to, and monitor risk over
6848  time. This strategy should clearly include any identified C-SCRM considerations and should
6849  result in the establishment of C-SCRM-specific processes throughout the agency. These
6850  processes should be documented in one of three ways:
6851
6852      1. Integrated into existing agency documentation;
6853      2. A separate set of documents addressing C-SCRM; or
6854      3. A mix of separate and integrated documents based on agency needs and operations.
6855

---

[30] Federal Departments' and Agencies' governance structures vary widely (see [NIST SP 800-100, Section 2.2.2]). Regardless of the governance structure, individual agency risk decisions should apply to the agency and any subordinate organizations, but not in the reverse direction.

6856 The following information should be provided as an output of the risk framing step, regardless of
6857 how the outputs are documented:
6858
6859    • C-SCRM Policy;
6860    • Criticality including prioritized mission and business processes and FIPS 199 impact;
6861    • Cyber supply chain risk assessment methodology and guidance;
6862    • Cyber supply chain risk response guidance;
6863    • Cyber supply chain risk monitoring guidance;
6864    • C-SCRM mission/business requirements;
6865    • Revised mission/business processes and enterprise architecture with C-SCRM
6866      considerations integrated;
6867    • Operational-level C-SCRM requirements; and
6868    • Acquisition security guidance/requirements.
6869
6870 Outputs from the risk framing step are enabling pre-requisites to effectively manage cyber
6871 supply chain risk and serve as inputs to the risk assessment, risk response, and risk monitoring
6872 steps.
6873
6874 **ASSESS**
6875 **Inputs and Preconditions**
6876
6877 Assess is the step where assumptions, established methodologies and collected data is used to
6878 conduct a risk assessment. Numerous inputs (including criticality, risk appetite and tolerance,
6879 threats, and vulnerability analysis results; stakeholder knowledge; and policy, constraints, and
6880 requirements) are combined and analyzed to gauge the likelihood and impact of a cyber supply
6881 chain compromise. Assess step activities are used to update the organizations long-term risk-
6882 framing assumptions to account for near-term variations and changes.
6883
6884 A cyber supply chain risk assessment should be integrated into the overall organization risk
6885 assessment process. C-SCRM risk assessment results should be used and aggregated as
6886 appropriate to communicate potential or actual cyber supply chain risks relevant to each risk
6887 management framework level. Figure 2-6 depicts the Assess Step with its inputs and outputs
6888 along the three levels.
6889
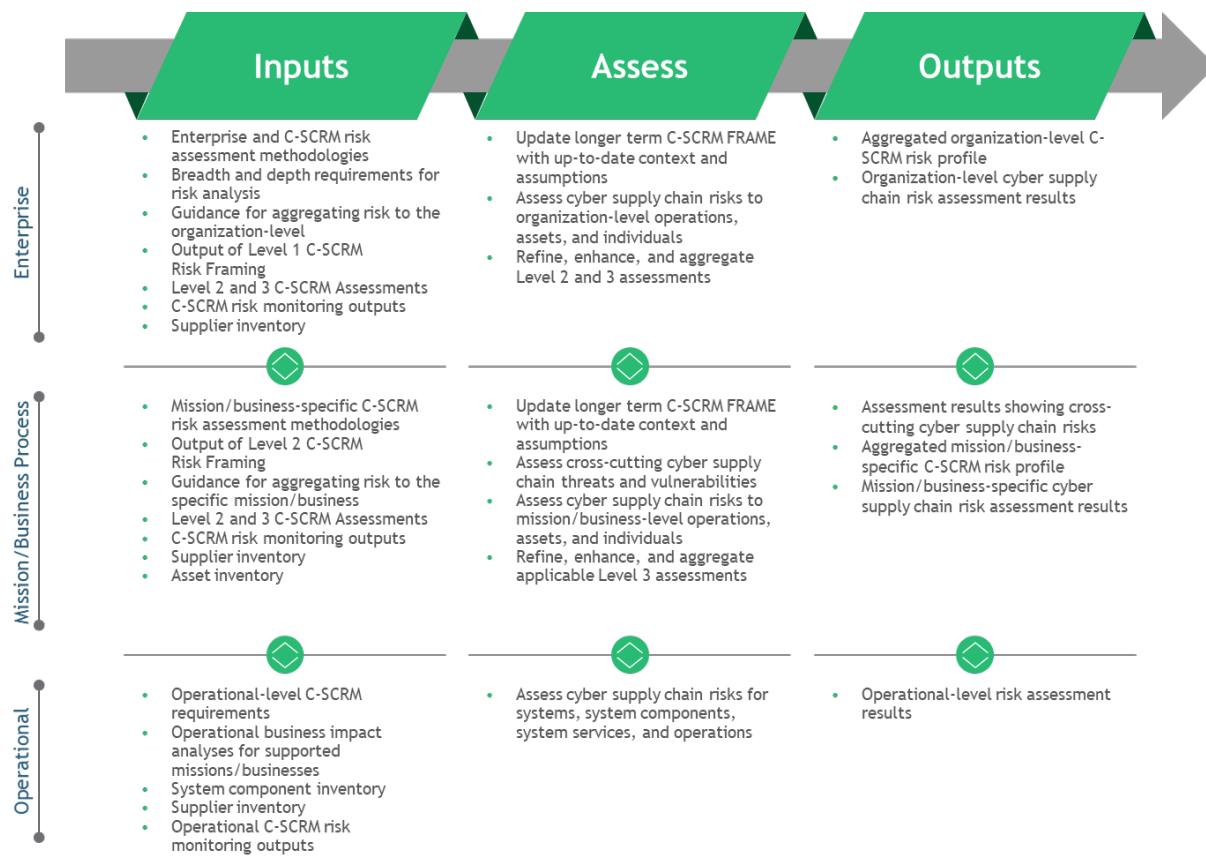
**Fig. C-3: C-SCRM in the Assess Step[31]**

Criticality, vulnerability, and threat analyses are essential to the supply chain risk assessment process. The order of activities begins with updating the criticality analysis to ensure the assessment is scoped to minimally include relevant critical mission and business processes and to understand the relevance and impact of cyber supply chain elements on these mission and business processes. As depicted in Figure C-4, vulnerability and threat analyses can then be performed, in any order, but should be performed iteratively to ensure that all applicable threats and vulnerabilities have been identified to understand which vulnerabilities may be more susceptible to exploitation by certain threats, and, if and as applicable, to associate identified vulnerabilities and threats to one or more mission and business processes or supply chain elements. Once viable threats and potential or actual vulnerabilities are assessed, this information will be used to evaluate the likelihood of exploitability—a key step to understanding impact. This is a synthesis point for criticality analysis, vulnerability analysis, and threat analysis and helps to further clarify and contextualize impact to support an informed and justifiable risk decision.

***Activities***

CRITICALITY ANALYSIS

---

[31] More detailed information on the Risk Management Process can be found in Appendix C

6911  **TASK 2-0:** Update Criticality Analysis of mission and business processes, systems, and system
6912  components to narrow the scope (and resource needs) for C-SCRM activities to those most
6913  important to mission success.
6914
6915  **Supplemental Guidance**

6916  Criticality analysis should include the cyber supply chain for both the organization and
6917  applicable suppliers, developers, system integrators, external system service providers, and other
6918  ICT/OT-related service providers, as well as relevant non-system services and products.
6919  Criticality analysis assesses the direct impact they each have on the mission priorities. The cyber
6920  supply chain includes the SDLC for applicable systems, services, and components because the
6921  SDLC defines whether security considerations are built into the systems/components or added
6922  after systems/components have been created.
6923
6924  Organizations should update and tailor criticality established during the Frame step of the risk
6925  management process, including FIPS 199 system. For low-impact systems, organizations should
6926  minimally assess criticality regarding interdependencies that systems may have with moderate or
6927  high-impact system(s). If systems are used extensively throughout the enterprise, organizations
6928  should determine the holistic impact of component failure or compromise in the low impact
6929  system.
6930
6931  In addition to updating and tailoring criticality, performing criticality analysis in the Assess Step
6932  may include the following:
6933
6934     •   Refine the dependency analysis and assessment to update understanding of which
6935         components may require hardening given the system or network architecture;
6936     •   Obtain and review existing information that the agency has about critical
6937         systems/components such as locations where they are manufactured or developed,
6938         physical and logical delivery paths, information flows and financial transactions
6939         associated with these components, and any other available information that can provide
6940         insights into cyber supply chain of these components;[32]
6941     •   Update information about the cyber supply chain, historical data, and the SDLC to
6942         identify changes in critical cyber supply chain paths and conditions.
6943
6944  The outcome of the updated criticality analysis is a narrowed, prioritized list of the
6945  organization's critical processes, systems, and system components as well as a refined
6946  understanding of corresponding dependencies within the supply chain. Organizations can use the
6947  Criticality process in Section 2.2.1, Task 1-1, to update Criticality Analysis.
6948
6949  Because more information will be available in the Assess step, organizations can narrow the
6950  scope and increase the granularity of a criticality analysis. When identifying critical processes
6951  and associated systems/components and assigning them criticality levels, consider the following:

---

[32] This information may be available from a supply chain map for the agency or individual IT projects or systems. Supply chain maps are descriptions or depictions of supply chains including the physical and logical flow of goods, information, processes, and money upstream and downstream through a supply chain. They may include supply chain entities, locations, delivery paths, or transactions.

- Functional breakdown is an effective method of identifying processes, associated critical components, and supporting defensive functions;
- Dependency analysis is used to identify the processes on which critical processes depend (e.g., defensive functions such as digital signatures used in software patch acceptance) which become critical processes themselves;
- Identification of all access points to identify and limit unmediated access to critical function/components (e.g., least-privilege implementation);
- Value chain analysis to understand inputs, process actors, outputs and customers of services and products; and
- Malicious alteration or other types of supply chain compromise can happen throughout the SDLC.

The resulting list of critical processes and supply chain dependencies is used to guide and inform the vulnerability analysis and threat analysis in determining the initial C-SCRM risk as depicted in Figure 2-3. Cyber supply chain countermeasures and mitigations can then be selected and implemented to reduce risk to acceptable levels.

Criticality analysis is performed iteratively and may be performed at any point in the SDLC and concurrently by level. The first iteration is likely to identify critical processes and systems/components that have a direct impact on mission and business processes. Successive iterations will include information from the criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies defined at each of the other levels. Each iteration will refine the criticality analysis outcomes and result in the addition of defensive functions. Several iterations are likely required to establish and maintain the criticality analysis results. Organizations should document or record the results of their criticality analysis and review and update this assessment on an annual basis at minimum.


THREAT AND VULNERABILITY IDENTIFICATION

**TASK 2-1:** Identify threats to and vulnerabilities in organizational information systems and the environments in which the systems operate.

**Supplemental Guidance**

In addition to threat and vulnerability identification, as described in [NIST SP 800-39] and [NIST SP 800-30 Rev. 1], organizations should conduct cyber supply chain threat analysis and vulnerability analysis.

*Threat Analysis*

For C-SCRM, a threat analysis provides specific and timely threat characterization of threat events (see Appendix C) and potential threat actors (e.g., Nation State) and threat vectors (e.g., 3rd party supplier), to inform management, acquisition, engineering, and operational activities

6997    within an organization.[33] A variety of information can be used to assess potential threats,
6998    including open source, intelligence, and counterintelligence. Organizations should include,
6999    update and refine the threat sources and assumptions defined during the *Frame* step. The results
7000    of the threat analysis will ultimately support acquisition decisions, alternative build decisions,
7001    and development and selection of appropriate mitigations to be applied in the *Respond* step. The
7002    focus of Cyber supply chain threat analysis should be based on the results of the criticality
7003    analysis.

7005    Agencies should use information available from existing incident management activities to
7006    determine whether they have experienced a cyber supply chain compromise and to further
7007    investigate such compromises. Agencies should define criteria for what constitutes a cyber
7008    supply chain compromise to ensure that such compromises can be identified as a part of post-
7009    incident activities, including forensics investigations. Additionally - at agency defined intervals –
7010    agencies should review other sources of incident information within the organization to
7011    determine whether in fact a supply chain compromise has occurred.

7013    An cyber supply chain threat analysis should capture at least the following data:
7014      • Observation of cyber supply chain-related attacks while they are occurring;
7015      • Incident data collected post-cyber supply chain-related compromise;
7016      • Observation of tactics, techniques, and procedures used in specific attacks, whether
7017        observed or collected using audit mechanisms; and
7018      • Natural and man-made disasters before, during, and after occurrence.

7021    *Vulnerability Analysis*

7023    For C-SCRM, a vulnerability is a weakness in an information system, system security
7024    procedures, internal controls, or implementation that could be exploited or triggered by a threat
7025    source [FIPS 200], [NIST SP 800-34 Rev. 1], [NIST SP 800-53 Rev 4], [NIST SP 800-53A Rev.
7026    4], [NIST SP 800-115].

7028    A vulnerability analysis is an iterative process that informs risk assessment and countermeasure
7029    selection. The vulnerability analysis works alongside the threat analysis to help inform the
7030    impact analysis and to help scope and prioritize vulnerabilities to be mitigated.

7032    Vulnerability analysis in the Assess Step should use the approaches defined during the Frame
7033    Step to update and refine assumptions about cyber supply chain vulnerabilities. Vulnerability
7034    analysis should begin by identifying vulnerabilities that are applicable to critical mission and
7035    business processes and systems/system components identified by the criticality analysis. An
7036    investigation of vulnerabilities may indicate the need to raise or at least reconsider the criticality
7037    levels of processes and components identified in earlier criticality analyses. Later iterations of

---

[33] Please note that threat characterization of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers may be benign.

7038 the vulnerability analysis may also identify additional threats, or opportunities for threats, not
7039 considered in earlier threat assessments.
7040
7041 Table C-8 provides examples of applicable cyber supply chain vulnerabilities that can be
7042 observed within the three levels.
7043
7044 **Table C-8: Examples of Cyber Supply Chain Vulnerabilities Mapped to the Organizational**
7045 **Levels**

| Level | Agency Constraints | Cyber Supply Chain Constraints |
|---|---|---|
| Level 1 – Organization | 1) Deficiencies or weaknesses in organizational governance structures or processes such as a lack of C-SCRM Plan<br>2) Weaknesses in the supply chain itself (e.g., vulnerable entities, over-reliance on certain entities) | 1) Provide guidance on how to consider dependencies on external organizations as vulnerabilities.<br>2) Seek out alternate sources of new technology including building in-house. leveraging trustworthy shared services/common solutions. |
| Level 2 – Mission/ Business | 1) No operational process is in place for detecting counterfeits<br>2) No budget was allocated for the implementation of a technical screening for acceptance testing of supplied system components entering the SDLC as replacement parts<br>3) Susceptibility to adverse issues from innovative technology supply sources (e.g., technology owned or managed by third parties is buggy) | 1) Develop a program for detecting tainted or counterfeit products and allocate appropriate budgets for putting in resources and training.<br>2) Allocate budget for acceptance testing – technical screening of components entering SDLC. |
| Level 3 – Operation | 1) Discrepancy in system functions not meeting requirements, resulting in substantial impact to performance | 1) Initiate engineering change. Malicious alteration can happen throughout the system life cycle to an agency system to address functional discrepancy and test correction for performance impact. |

7046
7047

7048    RISK DETERMINATION
7049
7050    **TASK 2-2:** Determine the risk to organizational operations and assets, individuals, other
7051    organizations, and the Nation if identified threats exploit identified vulnerabilities.
7052
7053    **Supplemental Guidance**
7054
7055    Organizations determine cyber supply chain risk by considering the likelihood that known threats
7056    exploit known vulnerabilities to and through the cyber supply chain and the resulting
7057    consequences or adverse impacts (i.e., magnitude of harm) if such exploitations occur.
7058    Organizations use threat and vulnerability information together with likelihood and
7059    consequences/impact information to determine C-SCRM risk either qualitatively or
7060    quantitatively. Outputs from the Risk Determination at Levels 1 and 2 should correspond directly
7061    with the RMF Prepare – Organization Level tasks described within [NIST 800-37r2], while risk
7062    assessments completed for Level 3 should correspond to directly with the RMF Prepare –
7063    Operational-level tasks.
7064
7065    *Likelihood*
7066
7067    Likelihood is a weighted factor based on a subjective analysis of the probability that a given
7068    threat is capable of exploiting a given vulnerability [CNSSI 4009]. Determining this likelihood
7069    requires the consideration of the characteristics of the threat sources, the identified
7070    vulnerabilities, and the organization's susceptibility to the cyber supply chain compromise, prior
7071    to and while the safeguards/mitigations are implemented. Likelihood determination should draw
7072    on methodologies defined as part of the Frame step, and update, refine, and expand any
7073    assumptions made about likelihood. For adversarial threats, this analysis should consider the
7074    degree of an adversary's capability and intent to interfere with the organization's mission. Cyber
7075    supply chain risk assessment should consider two views:
7076
7077    • The likelihood that one or more elements within the cyber supply chain itself is
7078      compromised. This may impact, for example, the availability of quality components or
7079      increase the risk of intellectual property theft; and
7080    • The likelihood of the system or component within the supply chain being compromised,
7081      for example, by malicious code inserted into a system or an electric storm damaging a
7082      component.
7083
7084    In some cases, these two views may overlap or be indistinguishable, but both may have an
7085    impact on the agency's ability to perform its mission.
7086
7087    Likelihood determination should consider:
7088
7089    • Threat assumptions that articulate the types of threats the system or the component may
7090      be subject to, such as cybersecurity threats, natural disasters, or physical security threats
7091    • Actual supply chain threat information such as adversaries' capabilities, tools, intentions,
7092      and targets

7093    • Historical data about the frequency of supply chain events in peer or like organizations
7094    • Internal expert perspectives on the probability systems or process compromise through
7095      the supply chain
7096    • Exposure of components to external access (i.e., outside of the system boundary)
7097    • Identified system, process, or component vulnerabilities
7098    • Empirical data on weaknesses and vulnerabilities available from any completed analysis
7099      (e.g., system analysis, process analysis) to determine probabilities of cyber supply chain
7100      threat occurrence
7101
7102    Factors for consideration include the ease or difficulty of successfully attacking through a
7103    vulnerability and the ability to detect the method employed to introduce or trigger a
7104    vulnerability. The objective is to assess the net effect of the vulnerability, which will be
7105    combined with threat information to determine the likelihood of successful attacks within a
7106    defined time frame as part of the risk assessment process. The likelihood can be based on threat
7107    assumptions or actual threat data, such as previous breaches of the supply chain, specific
7108    adversary capability, historical breach trends, or frequency of breaches. The organization may
7109    use empirical data and statistical analysis to determine specific probabilities of breach
7110    occurrence, depending on the type of data available and accessible within the organization.
7111
7112    *Impact*
7113
7114    Organizations should begin impact analysis using methodologies and potential impact
7115    assumptions defined during the Frame step, determining the impact of a compromise and the
7116    impact of mitigating said compromise. Organizations need to identify the various adverse
7117    impacts of compromise, including: (i) the characteristics of the threat sources that could initiate
7118    the events; (ii) identified vulnerabilities; and (iii) the organizational susceptibility to such events
7119    based on planned or implemented countermeasures. Impact analysis is an iterative process
7120    performed initially when a compromise occurs, when mitigation approach is decided to evaluate
7121    the impact of change, and finally, in the ever-changing SDLC, when the situation/context of the
7122    system or environment changes.
7123
7124    Organizations should use the result of impact analysis to define an acceptable level of cyber
7125    supply chain risk for a given system. Impact is derived from criticality, threat, and vulnerability
7126    analysis results, and should be based on the magnitude of effect on organizational operations,
7127    organizational assets, individuals, other organizations, or the Nation (including the national
7128    security interests of the United States) of a loss of confidentiality, integrity, or availability of
7129    information or an information system [NIST SP 800-53 Rev. 5]. Impact is likely to be a
7130    qualitative measure requiring analytic judgment. Executive/decision-makers use impact as an
7131    input into the risk-based decisions whether to accept, avoid, mitigate, or share the resulting risks
7132    and the consequences of such decisions.
7133
7134    Organizations should document the overall results of cyber supply chain risk assessments in risk
7135    assessment reports.[34] Cyber supply chain risk assessment reports should cover risks in all three

---

[34] See [NIST SP 800-30 Rev. 1 Appendix K] for a description of risk assessment reports.

7136   organizational levels as applicable. Based on the organizational structure and size, multiple cyber
7137   supply chain risk assessment reports may be required. Agencies are encouraged to develop
7138   individual reports at Level 1. For Level 2, agencies should integrate cyber supply chain risks into
7139   the respective mission-level Business Impact Assessments (BIA) and may want to develop
7140   separate mission-level cyber supply chain risk assessment reports. For Level 3, agencies may
7141   want to integrate cyber supply chain risks into the respective Risk Response Framework. Risk
7142   Response Frameworks at all three levels should be interconnected, reference each other when
7143   appropriate, integrate with the C-SCRM Plans, and comprise part of authorization packages.
7144
7145   *Aggregation*
7146
7147   Organizations may use risk aggregation to roll up several discrete or lower-level risks into a
7148   more general or higher-level risk [NIST SP 800-30 Rev. 1]. This is especially important for C-
7149   SCRM as organizations strive to understand their exposure to the cyber supply chain at
7150   operational-levels as well as at the relationship level (i.e., Level 1). Ultimately, organizations
7151   may wish to aggregate and normalize their C-SCRM risk assessment results with other enterprise
7152   risk assessments to develop an understanding of total risk exposure across risk types (e.g.,
7153   financial, operational, legal/regulatory). To ease this process, organizations should maximize
7154   inheritance of common frameworks and lexicons from higher-order risk processes (e.g.,
7155   enterprise risk management).
7156
7157   When dealing with discrete risks (i.e., non-overlapping), organizations can more easily develop a
7158   holistic understanding of aggregate Level 1 and 2 risk exposures. In many cases, however,
7159   organizations will find that risk assessments completed at lower levels contain overlapping
7160   estimates for likelihood and/or impact magnitude. In these cases, the sum of the pieces (i.e., risk
7161   exposure ratings at lower levels) is greater than the whole (i.e., aggregate risk exposure of the
7162   organization). To overcome these challenges, organizations can employ a variety of techniques.
7163   Organizations may elect to use visualizations or heat maps to demonstrate the likelihood and
7164   impact of risks relative to one another. When presenting aggregate risk as a number, organizations
7165   should ensure that assessments of risk produce discrete outputs by adopting mutually exclusive
7166   and collectively exhaustive (MECE) frameworks. MECE frameworks guide analysis of inputs
7167   (e.g., threats, vulnerabilities, impacts) and allow the organization to minimize overlapping
7168   assumptions and estimates. Instead of summing together risks from lower levels, organizations
7169   may elect to perform a new holistic assessment at an upper level leveraging the combined
7170   assessment results from lower levels. Doing so can help organizations avoid double counting of
7171   risk resulting in overestimation of their aggregate risk exposure. Organizations should apply
7172   discretion in aggregating risks so as to avoid risk aggregations that are difficult to explain (e.g.,
7173   combining highly differentiated scenarios into a single number).
7174
7175   Quantitative methods offer distinct advantages for risk aggregation. Through the use of
7176   probabilistic techniques (e.g., Monte Carlo methods, Bayesian analysis), organizations can
7177   combine similar risks into a single, easily understood figure (e.g., dollars) in a mathematically
7178   defensible manner. Mutually exclusive and collectively exhaustive frameworks remain an
7179   important requirement for quantitative methods.
7180
7181

7182 **Outputs and Post Conditions**
7183 This step results in:
7184
7185 • Confirmed mission and business process criticality;
7186 • Establishment of relationships between the critical aspects of the system's cyber supply
7187    chain infrastructure (e.g., SDLC) and applicable threats and vulnerabilities;
7188 • Understanding of the likelihood and the impact of a potential cyber supply chain
7189    compromise;
7190 • Understanding mission and system-specific risks;
7191 • Documented cyber supply chain risk assessments for mission processes and individual
7192    systems; and
7193 • Integration of relevant cyber supply chain risk assessment results into the organization
7194    risk management process.
7195

7196 **RESPOND**
7197 **Inputs and Preconditions**
7198
7199 Respond is the step in which the individuals conducting risk assessment will communicate the
7200 assessment results, proposed mitigation/controls options, and the corresponding acceptable level
7201 of risk for each proposed option to the decision makers. This information should be presented in
7202 a manner appropriate to inform and guide risk-based decisions. This will allow decision makers
7203 to finalize appropriate risk response based on the set of options and taking into account the
7204 corresponding risk factors of choosing the various options. Sometimes an appropriate response is
7205 to do nothing and to monitor the adversary's activities and behavior to better understand the
7206 tactics and to attribute the activities.
7207
7208 Cyber supply chain risk response should be integrated into the overall organization risk response.
7209 Figure C-5 depicts the Respond Step with its inputs and outputs along the three organizational
7210 levels.
7211
7212

7213
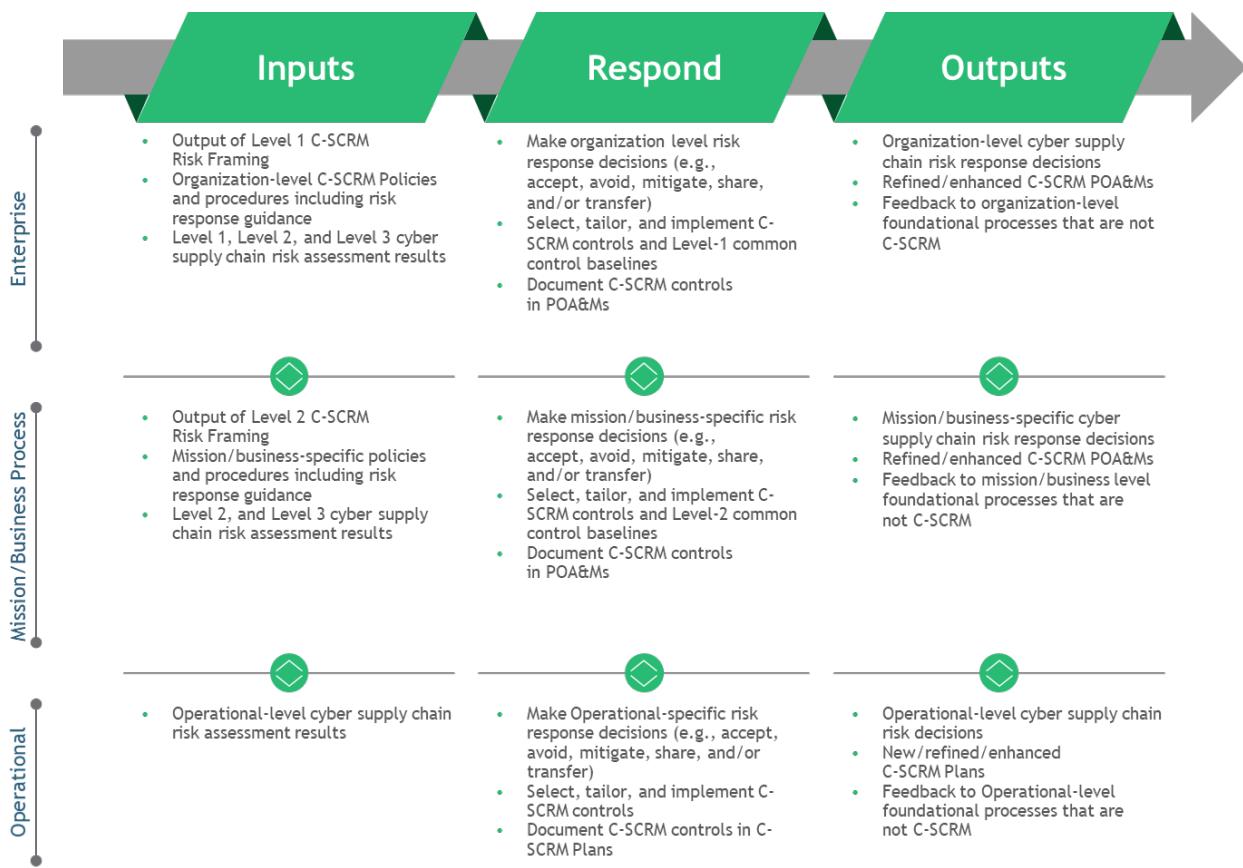
**Fig. C-4: C-SCRM in the Respond Step[35]**

7214

7215

7216    *Activities*

7217    RISK RESPONSE IDENTIFICATION

7218

7219    **TASK 3-1:** Identify alternative courses of action to respond to risk determined during the risk
7220    assessment.

7221

7222    Organization's risk response strategies will be informed by risk management strategies
7223    developed for the enterprise (i.e., Level 1) and mission/business process (i.e., Level 2). Risk
7224    response strategies will include general courses of action the organization may take as part of its
7225    risk response efforts (e.g., accept, avoid, mitigate, transfer or share). As part of mitigation efforts,
7226    organizations should select C-SCRM controls and tailor these controls based on the risk
7227    determination. C-SCRM controls should be selected for all three levels, as appropriate per
7228    findings of the risk assessments for each of the levels.

7229

7230    Many of the C-SCRM controls included in this document may be part of an IT security plan and
7231    should be incorporated as requirements in agreements made with third party providers. These
7232    controls are included because they apply to C-SCRM.

---

[35] More detailed information on the Risk Management Process can be found in Appendix C

7233
7234    This process should begin by determining acceptable risk to support the evaluation of
7235    alternatives (also known as trade-off analysis).
7236
7237    EVALUATION OF ALTERNATIVES
7238
7239    **TASK 3-2:** Evaluate alternative courses of action for responding to risk.
7240
7241    Once an initial acceptable level of risk has been defined, risk response courses of action should
7242    be identified and evaluated for efficacy in enabling the organization to achieve its defined risk
7243    threshold. Evaluation of alternatives typically occurs at Levels 1 or 2 with a focus on anticipated
7244    organization-wide impacts of C-SCRM to the organization's ability to successfully carry out
7245    organizational missions and processes. When carried out at Level 3, evaluation of alternatives
7246    will focus on the SDLC or the amount of time available for implementing the course of action.
7247
7248    Each courses of action analyzed may include a combination of risk acceptance, avoidance,
7249    mitigation, transfer and/or sharing. For example, an organization may elect to share a portion of
7250    its risk to a strategic supplier through the selection of controls included under contractual terms.
7251    Alternatively, an organization may choose to mitigate to acceptable levels though the selection
7252    and implementation of controls. In many cases, risk strategies will leverage a combination of risk
7253    response courses of action.
7254
7255    During evaluation of alternatives, organization will analyze available risk response courses of
7256    action for identified cyber supply chain risks. The goal of this exercise is to enable the
7257    organization to achieve an appropriate balance among C-SCRM and functionality needs of the
7258    organization. As a first step, organizations should ensure risk appetites and tolerances, priorities
7259    and tradeoffs, applicable requirements and constraints are reviewed with stakeholders familiar
7260    with broader organizational requirements, such as cost, schedule, performance, policy, and
7261    compliance. Through this process, the organization will identify risk response implications to the
7262    organization's broader requirements. Equipped with a holistic understanding of risk response
7263    implications, organizations should perform the C-SCRM, mission, and operational-level trade-
7264    off analyses to identify the correct balance of C-SCRM controls to respond to risk. At Level 3,
7265    the Frame, Assess, Respond, and Monitor process feeds into the RMF Select step described in
7266    [NIST SP 800-37 Rev. 2].
7267
7268    The selected C-SCRM controls for a risk response course of action will vary depending on where
7269    they are applied within organizational levels and SDLC processes. For example, C-SCRM
7270    controls may range from using a blind buying strategy to obscure end use of a critical
7271    component, to design attributes (e.g., input validation, sandboxes, and anti-tamper design). For
7272    each implemented control, the organization should identify someone responsible for its execution
7273    and develop a time- or event-phased plan for implementation throughout the SDLC. Multiple
7274    controls may address a wide range of possible risks. Therefore, understanding how the controls
7275    impact the overall risk is essential and must be considered before choosing and tailoring the
7276    combination of controls as yet another trade-off analysis may be needed before the controls can
7277    be finalized. The organization may be trading one risk for a larger risk unknowingly if the

7278 dependencies between the proposed controls and the overall risk are not well-understood and
7279 addressed.
7280
7281 RISK RESPONSE DECISION
7282
7283 **TASK 3-3:** Decide on the appropriate course of action for responding to risk.
7284
7285 As described in [NIST SP 800-39], organizations should select, tailor, and finalize C-SCRM
7286 controls, based on the evaluation of alternatives and an overall understanding of threats, risks,
7287 and supply chain priorities. Within Levels 1 and 2, the resulting decision, along with selected and
7288 tailored common control baselines (i.e., revisions to established baselines) should be documented
7289 within a C-SCRM-specific Risk Response Framework.[36] Within Level 3, the resulting decision,
7290 along with the selected and tailored controls, should be documented within the C-SCRM Plan as
7291 part of an authorization package.
7292
7293 Risk response decisions may be made by a risk executive or delegated by the risk executive to
7294 someone else in the organization. While the decision can be delegated to Level 2 or Level 3, the
7295 significance and the reach of the impact should determine the level at which the decision is being
7296 made. Risk response decisions may be made in collaboration with an organization's risk
7297 executives, mission owners, and system owners, as appropriate. Risk response decisions are
7298 heavily influenced by the organization's predetermined appetite and tolerance for risk. Using
7299 robust risk appetite and tolerance definitions, decision makers can ensure consistent alignment of
7300 the organization's risk decisions with its strategic imperatives. Robust definitions of risk appetite
7301 and tolerance may also enable organizations to delegate risk decision responsibility to lower
7302 levels of the organization and provide greater autonomy across the Levels.
7303
7304 Within Levels 1 and 2, the resulting decisions should be documented, along with any changes to
7305 requirements or selected common control baselines (enterprise or mission level), within C-
7306 SCRM-specific Risk Response Frameworks. The C-SCRM Risk Response Framework may
7307 influence other related Risk Response Frameworks.
7308
7309 The Risk Response Framework should include:
7310
7311 • Describing the threat source, threat event, exploited vulnerability, and threat event
7312   outcome;
7313 • Providing an analysis of the likelihood and impact of the risk and final risk score;
7314 • Describing the selected mitigating strategies and controls along with an estimate of the
7315   cost and effectiveness of the mitigation against the risk.
7316
7317 Within Level 3, the resulting decision, along with the selected and tailored controls, should be
7318 documented in a C-SCRM Plan. While the C-SCRM Plan is ideally developed proactively, it
7319 may also be developed in response to a cyber supply chain compromise. Ultimately, the C-
7320 SCRM Plan should cover the full SDLC, document a C-SCRM baseline, and identify cyber

---

[36] More information can be found on Risk Response Frameworks in Appendix B along with explicit examples.

supply chain requirements and controls at the Level 3 operational-level. The C-SCRM Plan
should be revised and updated based on the output of cyber supply chain monitoring.

C-SCRM Plans should:

- Summarize the environment as determined in Frame such as applicable policies,
  processes, and procedures based on organization and mission requirements currently
  implemented in the organization;
- State the role responsible for the plan such as Risk Executive, Chief Financial Officer
  (CFO), Chief Information Officer (CIO), Program Manager, or System Owner;
- Identify key contributors such as CFO, Chief Operations Officer (COO),
  Acquisition/Contracting, Procurement, C-SCRM PMO, System Engineer, System
  Security Engineer, Developer/Maintenance Engineer, Operations Manager, or System
  Architect;
- Provide the applicable (per level) set of risk mitigation measures and controls resulting
  from the Evaluation of Alternatives (in Respond);
- Provide tailoring decisions for selected controls including the rationale for the decision;
- Describe feedback processes among the levels to ensure that cyber supply chain
  interdependencies are addressed;
- Describe monitoring and enforcement activities (including auditing if appropriate)
  applicable to the scope of each specific C-SCRM Plan;
- If appropriate, state qualitative or quantitative measures to support implementation of the
  C-SCRM Plan and assess effectiveness of this implementation;[37]
- Define frequency for deciding whether the plan needs to be reviewed and revised;
- Include criteria that would trigger revision, for example, life cycle milestones, gate
  reviews, or significant contracting activities; and
- Include suppliers, developers, system integrators, external system service providers, and
  other ICT/OT-related service providers C-SCRM Plans if made available as part of
  agreements.

Agencies may want to integrate C-SCRM controls into the respective System Security Plans or
develop separate operational-level C-SCRM Plans. At Level 3, the C-SCRM Plan applies to
High and Moderate Impact systems per [FIPS 199]. Requirements and inputs from the Enterprise
C-SCRM strategy at Level 1, and Mission C-SCRM strategy and implementation plan at Level 2,
should flow down and be used to guide the develop C-SCRM Plans at Level 3. Conversely, the
C-SCRM controls and requirements at Level 3 should be considered in developing and revising
requirements and controls applied at the higher levels. C-SCRM Plans should be interconnected
and reference each other when appropriate.

Table 2-7 summarizes the controls to be contained in Risk Response Frameworks at Levels 1 and
2, and C-SCRM Plans at Level 3 and provides examples of those controls.

---

[37] NIST SP 800-55 Revision 1, *Performance Measurement Guide for Information Security* (July 2008)*,* provides guidance on
developing information security measures. Agencies can use general guidance in that publication to develop specific measures
for their C-SCRM plans. See http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

7361
7362 **Table C-9: Controls at Levels 1,2, and 3**

| Level | Controls | Examples |
|---|---|---|
| Level 1 | Provides organization common controls baseline to Levels 2 and 3 | • Minimum sets of controls applicable to all suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.<br>• Enterprise-level controls applied to processing and storing suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers information.<br>• Cyber supply chain training and awareness for acquirer staff at the enterprise-level. |
| Level 2 | • Inherits common controls from Level 1<br>• Provides mission and business process0level common controls baseline to Level 3<br> Provides feedback to Level 1 about what is working and what needs to be changed | • Minimum sets of controls applicable suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers for the specific mission and business process.<br>• Program-level refinement of Identity and Access Management controls to address C-SCRM concerns.<br>• Program-specific supply chain training and awareness. |
| Level 3 | • Inherits common controls from Levels 1 and 2<br>• Provides system-specific controls for Level 3<br> Provides feedback to Level 2 and Level 1 about what is working and what needs to be changed | • Minimum sets of controls applicable to service providers or specific hardware and software for the individual system.<br>• Appropriately rigorous acceptance criteria for change management for systems that support supply chain, e.g., as testing or integrated development environments.<br>• System-specific cyber supply chain training and awareness.<br>• Intersections with the SDLC. |

7363
7364 Appendix C provides an example C-SCRM Plan template with the sections and types of
7365 information organizations should include in their C-SCRM Planning activities.
7366
7367 RISK RESPONSE IMPLEMENTATION
7368 **TASK 3-4:** Implement the course of action selected to respond to risk.
7369
7370 Organizations should implement the C-SCRM Plan in a manner that integrates the C-SCRM
7371 controls into the overall agency risk management processes.

7372
7373 **Outputs and Post Conditions**
7374
7375 The output of this step is a set of C-SCRM controls that address C-SCRM requirements and can
7376 be incorporated into the system requirements baseline and in agreements with third-party
7377 providers. These requirements and resulting controls will be incorporated into the SDLC and
7378 other organizational processes, throughout the three levels.
7379
7380 For general risk types, this step results in:
7381 • Selected, evaluated, and tailored C-SCRM controls that address identified risks;
7382 • Identified consequences of accepting or not accepting the proposed mitigations; and
7383 • Development and implementation of the C-SCRM Plan.
7384
7385 **MONITOR**
7386 **Inputs and Preconditions**
7387
7388 Monitor is the step in which organizations: (i) verify compliance; (ii) determine the ongoing
7389 effectiveness of risk response measures; and (iii) identify risk-impacting changes to
7390 organizational information systems and environments of operation.
7391
7392 Changes to the organization, mission/business, operations, or the supply chain can directly
7393 impact the organization's cyber supply chain. The Monitor step provides a mechanism for
7394 tracking such changes and ensuring they are appropriately assessed for impact (in Assess). If the
7395 cyber supply chain is redefined as a result of monitoring, organizations should coordinate with
7396 the suppliers, developers, system integrators, external system service providers, and other
7397 ICT/OT-related service providers to resolve implications and mutual obligations.
7398
7399 Organizations should integrate C-SCRM into existing continuous monitoring programs.[38] In the
7400 event a Continuous Monitoring program does not exist, C-SCRM can serve as a catalyst for
7401 establishing a comprehensive continuous monitoring program. Figure 2-8 depicts the Monitor
7402 Step with inputs and outputs along the three organizational levels.
7403
7404
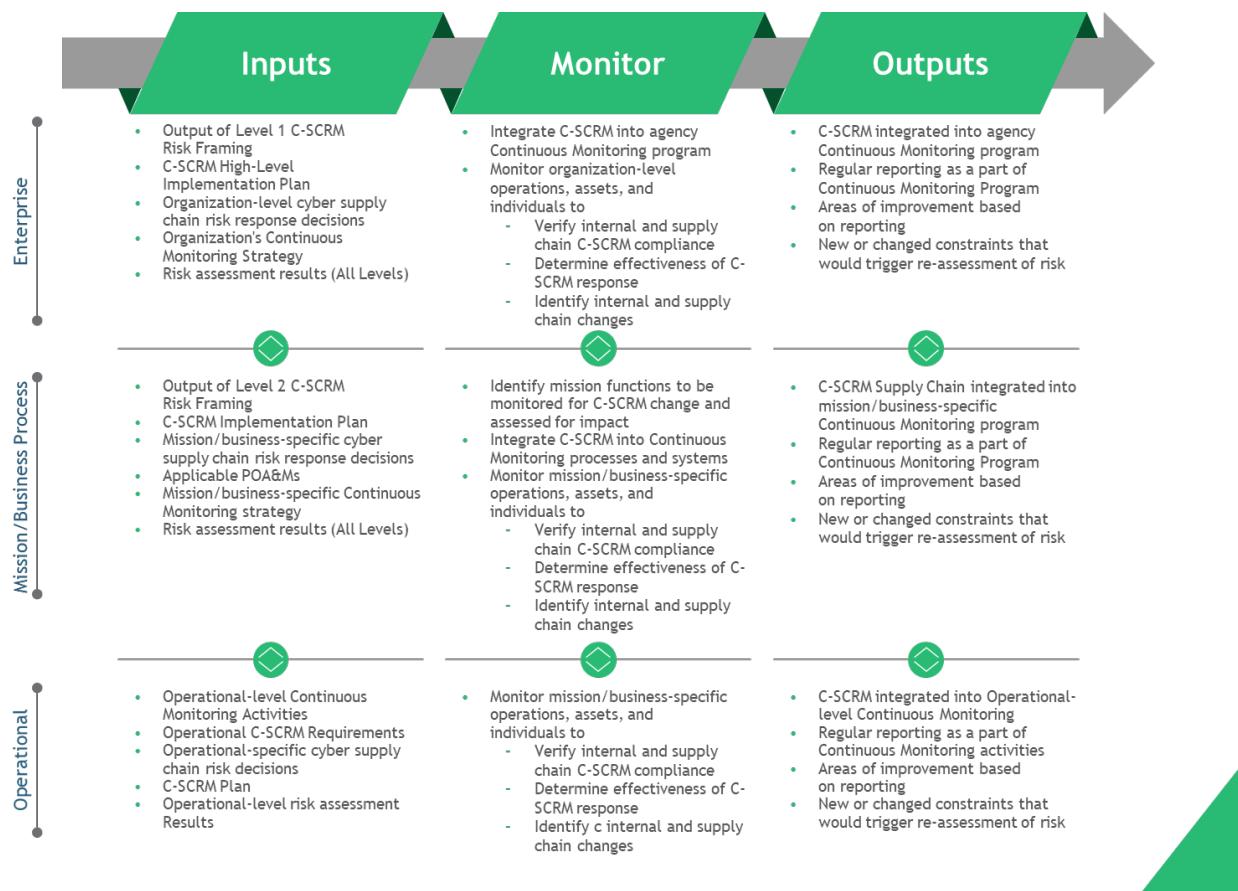
---

[38] NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*
(September 2011), describes how to establish and implement a continuous monitoring program. See
http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf.

7405
7406    **Fig. C-5: C-SCRM in the Monitor Step[39]**

7407
7408    *Activities*
7409    RISK MONITORING STRATEGY

7410    **TASK 4-1:** Develop a risk monitoring strategy for the organization that includes the purpose,
7411    type, and frequency of monitoring activities.
7412
7413    **Supplemental Guidance**
7414
7415    Organizations should integrate C-SCRM considerations into their overall risk monitoring
7416    strategy. Monitoring cyber supply chain risk may require access to information that agencies
7417    may not have traditionally collected. Some of the information will require needing to be gathered
7418    from outside the agency, such as from open sources or suppliers and integrators. The strategy
7419    should, among other things, include the data to be collected, state the specific measures compiled
7420    from the data (e.g., number of contractual compliance violations by the vendor), identify existing
7421    or include assumptions about required tools needed to collect the data, identify how the data will
7422    be protected, and define reporting formats for the data. Potential data sources may include:
7423    • Agency vulnerability management and incident management activities;
7424    • Agency manual reviews;

---

[39] More detailed information on the Risk Management Process can be found in Appendix C

- Interagency information sharing;
- Information sharing between the agency and suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers;
- Supplier information sharing; and
- Contractual reviews of suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers.

Organizations should ensure the appropriate protection of supplier data if that data is collected and stored by the agency. Agencies may also require additional data collection and analysis tools to appropriately evaluate the data to achieve the objective of monitoring applicable cyber supply chain risks.

RISK MONITORING

**TASK 4-2:** Monitor organizational information systems and environments of operation on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.

According to [NIST SP 800-39], organizations should monitor compliance, effectiveness, and change. Monitoring compliance within the context of C-SCRM involves monitoring an organization's processes and supplied products and services for compliance with the established security and C-SCRM requirements. Monitoring effectiveness involves monitoring the resulting risks to determine whether these established security and C-SCRM requirements produce the intended results. Monitoring change involves monitoring the environment for any changes that would signal changing requirements and mitigations/controls to maintain an acceptable level of cyber supply chain risk.

To monitor changes, organizations need to identify and document the set of triggers that would change cyber supply chain risk. While the categories of triggers will likely include changes to constraints, identified in Table 2-6 (during the Frame Step), such as policy, mission, change to the threat environment, enterprise architecture, SDLC, or requirements, the specific triggers within those categories may be substantially different for different organizations.

An example of a cyber supply chain change is two key vetted suppliers[40] announcing their departure from a specific market, therefore creating a supply shortage for specific components. This would trigger the need to evaluate whether reducing the number of suppliers could create vulnerabilities in component availability and integrity. In this scenario, potential deficit of components may result simply from insufficient supply of components, because fewer components are available. If none of the remaining suppliers are vetted, this deficit may result in uncertain integrity of the remaining components. If the organizational policy directs use of vetted components, this event may result in the organization's inability to fulfill its mission needs.

---

[40] A vetted supplier is a supplier with whom the organization is comfortable doing business. This level of comfort is usually achieved through developing an organization-defined set of supply chain criteria and then *vetting* suppliers against those criteria.

7467    In addition to regularly updating existing risks assessments with the results of the ongoing
7468    monitoring, the organization should determine the triggers of a reassessment. Some of these
7469    triggers may include availability of resources, changes to cyber supply chain risk, natural
7470    disasters, or mission collapse.
7471
7472    **Outputs and Post Conditions**
7473
7474    Organizations should integrate the cyber supply chain outputs of the Monitor Step into the C-
7475    SCRM Plan. This plan will provide inputs into iterative implementations of the Frame, Assess,
7476    and Respond Steps as required.
7477
7478
7479

**APPENDIX D: C-SCRM TEMPLATES**

**1.   C-SCRM STRATEGY & IMPLEMENTATION PLAN**

To address supply chain risks, organizations develop a C-SCRM strategy. The C-SCRM strategy, accompanied by an implementation plan, is at the enterprise level (Level1), though different mission/business areas (Level 2) may further tailor the C-SCRM strategy to address specific mission/business needs as outlined at the organizational level. The C-SCRM strategy and implementation plan should anchor to the overarching enterprise risk management strategy and comply with applicable laws, executive orders, directives, and regulations.

Typical components of the strategy and implementation plan, as outlined in the below template, include strategic approaches to reducing an organization's supply chain risk exposure via enterprise-wide risk management requirements, ownership, risk tolerance, roles and responsibilities, and escalation criteria.

**1.1. C-SCRM Strategy & Implementation Plan Template**

**1.1.1.   Purpose**

*Outline the organization's high-level purpose for the strategy and implementation document, aligning that purpose to organizational mission, vision, and values. Describe where the strategy and implementation document resides relative to other C-SCRM documentation that must be maintained at various tiers. Provide clear direction around the organization's C-SCRM priorities and its general approach for achieving those priorities.*

**Sample Text**

The purpose of this strategy and implementation document is to provide a strategic roadmap for implementing effective C-SCRM capabilities, practices, processes, and tools within the organization and in support of its vision, mission, and values.

The strategic approach is organized around a set of objectives that span the scope of the organization's mission and reflect a phased, achievable strategic approach to ensure successful implementation and effectiveness of C-SCRM efforts across the enterprise.

This strategy and implementation document discusses the necessary core functions, roles, and responsibilities, and the approach the organization will take to implement C-SCRM capabilities within the enterprise. As mission/business policies and system plans are developed and completed, they will be incorporated as attachments to this document. All three tiers of documentation should be periodically reviewed together to ensure cohesion and consistency.

The focus of this strategy and implementation plan is intentionally targeted toward establishing a core foundational capability. These baseline functions, such as defining policies, ownership, and dedicated resources will ensure the organization can expand and mature its C-SCRM capabilities over time.  This plan also acknowledges and emphasizes the need to raise awareness and ensure training for staff in order to understand C-SCRM and grow the competencies necessary to be able to perform C-SCRM functions.

This initial strategy and implementation plan also recognizes the dependencies on industry-wide coordination efforts, processes, and decisions. As government and industry-wide direction, process guidance, and requirements are clarified and communicated, the organization will update and refine its strategy and operational implementation plans and actions.

### 1.1.2. Authority & Compliance

*List of the laws, executive orders, directives, regulations, policies, standards, and guidelines that govern C-SCRM Strategy and Implementation.*

**Sample Text**

- Legislation
    - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018
    - Federal Information Security Modernization Act of 2014
    - Section 889 of the 2019 National Defense Authorization Act - "Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment"
    - Gramm-Leach-Bliley Act
    - Health Insurance Portability and Accountability Act
- Regulations
    - NYDFS 23 NYCRR 500: Section 500.11 Third Party Service Provider Security Policy
    - CIP-013-1: Cyber Security - Supply Chain Risk Management
    - FFIEC Information Security Handbook II.C.20: Oversight of Third-Party Service Providers
- Guidelines
    - NIST 800-53 Revision 5: CA-5, SR-1, SR-2, SR-3
    - NIST 800-37 Revision 2
    - NIST 800-161 Revision 1: Appendix C
    - ISO 28000:2007

### 1.1.3. Strategic Objectives

*Strategic objectives establish the foundation for determining enterprise-level C-SCRM controls and requirements. Each objective supports achievement of the organization's stated purpose in pursuing sound C-SCRM practices and risk-reducing outcomes. Together, the objectives provide the organization with the essential elements needed to bring C-SCRM capabilities to life, and effectively pursue the organization's purpose.*

In aggregate, strategic objectives should address essential C-SCRM capabilities and enablers, such as:

- Implementing a risk management hierarchy and risk management approach;
- Establishing an organization governance structure that integrates C-SCRM requirements and incorporates these requirements into organizational policies;
- Defining a supplier risk assessment approach;

- Implementing a quality and reliability program that includes quality assurance and quality control process and practices;
- Establishing explicit collaborative roles, structures, and processes for supply chain, cybersecurity, product security, and physical security (and other relevant) functions;
- Ensuring that adequate resources are dedicated and allocated to information security and C-SCRM to ensure proper implementation of policy, guidance, and controls;
- Implementing a robust incident management program to successfully identify, respond to, and mitigate security incidents; and
- Including key suppliers in contingency planning, incident response, and disaster recovery planning and testing.

**Sample Text**

**Objective 1: Effectively manage cyber supply chain risks**

This objective addresses the primary intent of the organization's pursuit of C-SCRM. The establishment and sustainment of an enterprise-wide C-SCRM program will enable the organization's risk owners to identify, assess, and mitigate supply chain risk to the organization's assets, functions, and associated services. Implementing an initial capability that can sustain and grow in its scope of focus and breadth and depth of functions will be done in phases and will consider holistic "people, process, and technology" needs to ensure the organization is able to achieve desired C-SCRM goals in areas such as improving enterprise awareness, protection, and resilience.

**Objective 2: Serve as a trusted source of supply for customers**

Addressing customer supply chain risks at scale and across the organization's diverse portfolio demands a prioritization approach, structure, improved processes, and ongoing governance. C-SCRM practices and controls need to be tailored to address the distinct and varied supply chain threats and vulnerabilities that are applicable for the organization's customers. This objective can be achieved by:
- Strengthening vetting processes, C-SCRM requirements, and oversight of external providers;
- Ensuring customer needs are met in line with their cyber supply chain risk appetite, tolerance, and environment.

**Objective 3: Position as an industry leader in C-SCRM**

The organization is well-positioned to enable and drive improvements forward in addressing how cyber supply chain risks across the industry. Therefore, we must use this position to advocate with industry stakeholders about communication, incentivization, and education of industry players about our requirements and expectations related to addressing supply chain risk.

7607    **1.1.4.  Implementation Plan & Progress Tracking**
7608
7609    *Outline the methodology and milestones by which progress against the enterprise's C-SCRM*
7610    *strategic objectives will be tracked. Though organizational context heavily informs this process,*
7611    *organizations should define prioritized time horizons to encourage execution of tasks critical or*
7612    *foundational in nature. Common nomenclature for defining such time horizons includes "crawl,*
7613    *walk, run" or "do now, do next, do later." Regardless of the time horizon designated,*
7614    *implementation of practical, prioritized plans is essential to building momentum in the*
7615    *establishment or enhancement of C-SCRM capabilities.*
7616
7617    Once the implementation plan is baselined, an issue escalation process and feedback mechanism
7618    is included that drives changes to the implementation plan and progress tracking.
7619

7620    **Sample Text**

7621    [Organization's] execution of its C-SCRM strategic objectives and sustained operational
7622    effectiveness of underlying activities requires a formal approach and commitment to progress
7623    tracking. [Organization] will track and assess implementation of its strategic objectives by
7624    defining subsidiary milestones and implementation dates in an implementation plan. Monitoring
7625    and reporting against implementation plan requires shared responsibility across multiple
7626    disciplines and requires a cross-organization, team-based approach.
7627
7628    The following implementation plan will be continuously maintained by mission/business owners
7629    and reviewed by the Senior Leadership team as a part of regular oversight activities.
7630
7631    Risks and issues impacting the implementation plan should be raised proactively by
7632    mission/business owners, or their team, to the Senior Leadership Team. The implementation plan
7633    may then be revised in accordance with Senior Leadership Team's discretion.
7634

| Objective 1: Effectively manage cyber supply chain risks | | | | |
|---|---|---|---|---|
| Implementation Plan Milestone | Status | Owner | Priority | Target Date |
| Establish policy and authority | Planned | J. Doe | Do Now | XX/XX/XX |
| Establish and provide executive oversight and direction | Complete | … | Do Next | … |
| Integrate C-SCRM into enterprise risk management (ERM) framework | Delayed | … | Do Later | … |
| Establish C-SCRM PMO capability and organization | Cancelled | … | … | … |
| Establish roles, responsibilities, and assign accountability | … | … | … | … |
| Develop C-SCRM plans | … | … | … | … |
| Stand up internal awareness function | … | … | … | … |

| | | | | |
|---|---|---|---|---|
| Identify, prioritize, and implement supply chain risk assessment capabilities | … | … | … | … |
| Establish, document, and implement enterprise-level C-SCRM controls | … | … | … | … |
| Identify C-SCRM resource requirements and secure sustained funding | … | … | … | … |
| Establish C-SCRM program performance monitoring | … | … | … | … |

7635

| **Objective 2: Serve as a trusted source of supply for customers** | | | | |
|---|---|---|---|---|
| Implementation Plan Milestone | Status | Owner | Priority | Target Date |
| Incorporate C-SCRM activities customer-facing business lines, programs, and solution offerings | Planned | J. Doe | Do Now | XX/XX/XX |
| Ensure customer support personnel are well versed in cyber supply chain risks and management requirements | Complete | … | Do Next | … |
| Establish minimum baseline levels of cyber supply chain assurance | Delayed | … | Do Later | … |
| Establish processes to respond to identified risks and to monitor for impacts to the organization's cyber supply chain | Cancelled | … | … | … |

7636

| **Objective 3: Position as an industry leader in C-SCRM** | | | | |
|---|---|---|---|---|
| Implementation Plan Milestone | Status | Owner | Priority | Target Date |
| Coordinate and engage with national security and law enforcement to ensure rapid access to mission-critical supply chain threats | Planned | J. Doe | Do Now | XX/XX/XX |
| Evaluate C-SCRM improvement opportunities and strengthen requirements and oversight for industry-wide common solutions / shared services | Complete | … | Do Next | … |
| Advocate for C-SCRM awareness and competency through training and workforce development | Delayed | … | Do Later | … |
| Release whitepapers and public guidance related to C-SCRM | Cancelled | … | … | … |

7637
### 1.1.5. Roles & Responsibilities

7639

*Assign those responsible for the Strategy & Implementation template, as well as its key contributors. Include the role and name of each individual or group, as well contact information where necessary (e.g., organizational affiliation, address, email address, and phone number).*

7643
**Sample Text**

- Senior Leadership Team shall:
  - endorse the enterprise's C-SCRM strategic objectives and implementation plan
  - provide oversight of C-SCRM implementation and effectiveness
  - communicate C-SCRM direction and decisions for priorities and resourcing needs
  - determine the enterprise's risk appetite and risk tolerance; and
  - respond to high-risk C-SCRM issue escalations that could impact the organization's risk posture in a timely manner.

- Mission/Business Owners shall:
  - determine mission level risk appetite and tolerance, ensuring they are in line with enterprise expectations
  - define supply chain risk management requirements and implementation of controls that support enterprise objectives
  - maintain criticality analyses of mission functions and assets; and
  - perform risk assessments for mission/business-related procurements.

7660
### 1.1.6. Definitions

7662

*List the key definitions described within the Strategy & Implementation template, providing organizationally specific context and examples where needed.*

7665
**Sample Text**

- Enterprise: An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information, and mission management.

- Objective: An organization's broad expression of goals. Specified target outcome for operations.

7675
### 1.1.7. Revision & Maintenance

7676

*Define the required frequency of Strategy & Implementation template revisions. Maintain a table of revisions to enforce version control. Strategy & Implementation templates are living documents that must be updated and communicated to all appropriate individuals (e.g., staff, contractors, and suppliers).*

7681
**Sample Text**

[Organization's] Strategy & Implementation template must be reviewed at a minimum every 3-5 years (within the federal environment) since changes to laws, policies, standards, guidelines, and controls are dynamic and evolving. Additional criteria that may trigger interim revisions include:

- change of policies that impact the Strategy & Implementation template;
- significant Strategy & Implementation events;
- introduction of new technologies;
- discovery of new vulnerabilities;
- operational or environmental changes;
- shortcomings in the Strategy & Implementation template;
- change of scope; and
- other organization-specific criteria.

**Sample Version Management Table**

| Version Number | Date | Description of Change/Revision | Section/Pages Affected | Changes made by Name/Title/Organization |
|---|---|---|---|---|
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

7699 **2. C-SCRM POLICY**
7700

7701 The C-SCRM policies direct the implementation of the C-SCRM strategy. C-SCRM policies can
7702 be developed at Level 1 and/or at Level 2 and are informed by the mission/business specific
7703 factors, including risk context, risk decisions and risk activities from the C-SCRM strategy. The
7704 C-SCRM policies support applicable organizational policies (e.g., acquisition and procurement,
7705 information security and privacy, logistics, quality, and supply chain). The C-SCRM policies
7706 address the goals and objectives outlined in the organization's C-SCRM strategy, which in turn
7707 is informed by the organization's strategic plan. The C-SCRM policies should also address
7708 missions and business functions, and the internal and external customer requirements. C-SCRM
7709 policies also define the integration points for C-SCRM with the risk management and processes
7710 for the organization. Finally, the C-SCRM policies define at a more specific and granular level
7711 the C-SCRM roles and responsibilities within the organization, any interdependencies among
7712 those roles, and the interaction among the roles; the C-SCRM policies at Level 1 are more broad-
7713 based, whereas the C-SCRM policies at Level 2 are specific to the mission/business function. C-
7714 SCRM roles specify the responsibilities for procurement, conducting risk assessments, collecting
7715 supply chain threat intelligence, identifying and implementing risk-based mitigations,
7716 performing monitoring, and other C-SCRM functions.

7717 **2.1. C-SCRM Policy Template**
7718

7719 **2.1.1. Authority & Compliance**
7720
7721 *List of the laws, executive orders, directives, regulations, policies, standards, and guidelines that*
7722 *govern the C-SCRM policy.*
7723
7724 **Sample Level 1 Text**

7725 • Policies
7726   o [Organization Name] Enterprise Risk Management Policy
7727   o [Organization Name] Information Security Policy
7728 • Legislation
7729   o Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
7730     Technology Act (SECURE) Technology of 2018
7731 • Regulations
7732   o NYDFS 23 NYCRR 500: Section 500.11 Third Party Service Provider Security
7733     Policy
7734   o CIP-013-1: Cyber Security - Supply Chain Risk Management
7735   o FFIEC Information Security Handbook II.C.20: Oversight of Third-Party Service
7736     Providers
7737
7738 **Sample Level 2 Text**

7739 • Policies
7740   o [Organization Name] C-SCRM Policy

7741          o   [Mission and Business Process Name] Information Security Policy
7742     •   Regulations
7743          o   NYDFS 23 NYCRR 500: Section 500.11 Third Party Service Provider Security
7744              Policy
7745     •   Guidelines
7746          o   NIST 800-53 Revision 5: SR-1, PM-9, PM-30, PS-8, SI-12
7747          o   NIST 800-161 Revision 1: Appendix C
7748

### 2.1.2.  Description

7750
7751 *Describe the purpose and scope of the C-SCRM policy, outlining the organizational leaderships'*
7752 *intent to adhere to the plan, enforce its controls, and ensure that it remains current. Define the*
7753 *tier(s) at which the policy applies. C-SCRM policies may need to be derived in whole or in part*
7754 *from existing policies or other guidance.*
7755
7756 *For Level 2 C-SCRM policies should list all Level 1 policies and plans that inform the Level 2*
7757 *policies, provide a brief explanation of what this mission/business encompasses and briefly*
7758 *describe the scope of applicability (e.g. plans, systems, type of procurements, etc.) for these*
7759 *Level 2 C-SCRM policies.*
7760

**Sample Level 1 Text**

7762
7763 [Organization] is concerned about the risks in the products, services, and solutions bought, used,
7764 and offered to customers.
7765
7766 The policy objective of the [Organization's] C-SCRM Program is to successfully implement and
7767 sustain the capability of providing improved assurance that the products, services, and solutions
7768 used and offered by [Organization] are trustworthy, appropriately secure and resilient, and able
7769 to perform to the required quality standard.
7770
7771 C-SCRM is a systematic process for identifying and assessing susceptibilities, vulnerabilities,
7772 and threats throughout the supply chain and implementing strategies and mitigation controls to
7773 reduce risk exposure and combat threats. The establishment and sustainment of an enterprise-
7774 wide C-SCRM Program will enable [Organization's] risk owner(s) to identify, assess, and
7775 mitigate supply chain risk to [Organization's] mission assets, functions, and associated services.
7776

**Sample Level 2 Text**

7778
7779 [Mission and Business Process] recognizes its criticality to [Organization Objective]. A key
7780 component of producing products involves coordinating among multiple suppliers, developers,
7781 system integrators, external system service providers, and other ICT/OT-related service
7782 providers. [Mission and Business Process] understands the realization of cyber supply chain risks
7783 may disrupt or completely inhibit [Mission and Business Process]'s ability to generate products
7784 in a timely manner and in accordance with the required quality standard.
7785

7786　Based on the C-SCRM objectives set forth by [Organization Level 1 Policy Name], [Mission and
7787　Business Process]'s policy objective is to implement C-SCRM capabilities allowing for the
7788　assessment, response, and monitoring of cyber supply chain risks. C-SCRM capabilities that
7789　align with the policy and requirements set forth by the enterprise-wide C-SCRM program will
7790　provide the boundaries within which [Mission and Business Process Name] will tailor C-SCRM
7791　processes and practices to meet the unique requirements associated with sourcing components
7792　and assembling key products.
7793

7794　**2.1.3. Policy**
7795

7796　*Outline the mandatory high-level policy statements that underpin the goals and objectives of the*
7797　*C-SCRM organization's strategic plan, missions and business functions, and the internal and*
7798　*external customer requirements.*
7799

7800　**Sample Level 1 Text**

7801　[Organization's] enterprise-level C-SCRM Program is established to implement and sustain the
7802　capability to:
7803　　　• assess and provide appropriate risk response to cyber supply chain risk posed by the
7804　　　　acquisition and use of covered articles;
7805　　　• prioritize cyber supply chain risk assessments and risk response actions based on
7806　　　　criticality assessment of mission, system, component, service, or asset;
7807　　　• develop an overall C-SCRM strategy and high-level implementation plan and policies
7808　　　　and processes;
7809　　　• integrate supply chain risk management practices throughout the acquisition and asset
7810　　　　management life cycle of covered articles;
7811　　　• share C-SCRM information in accordance with industry-wide criteria and guidelines; and
7812　　　• guide and oversee implementation progress and program effectiveness.
7813

7814　The C-SCRM Program shall:
7815　　　• be centrally led and coordinated by a designated senior leadership who shall function as
7816　　　　the [Organization's] C-SCRM Program Executive and chair the C-SCRM Program
7817　　　　Management Office (PMO);
7818　　　• leverage and be appropriately integrated into existing [Organization's] risk-management
7819　　　　and decision-making governance processes and structures;
7820　　　• reflect a team-based approach and be collaborative, interdisciplinary, and intra-
7821　　　　organizational in nature and composition;
7822　　　• incorporate a Leveled risk management approach, consistent with the NIST Risk
7823　　　　Management Framework and NIST's supply chain risk management Special Publication
7824　　　　800-161 Revision 1; and
7825　　　• implement codified and regulatory C-SCRM requirements and industry-wide and
7826　　　　[Organization]-specific policy direction, guidance, and processes.
7827

7828　**Sample Level 2 Text**

7829　[Mission and Business Process]'s C-SCRM Program shall:

- operate in accordance with requirements and guidance set forth by [Organization] C-SCRM Program
- collaborate with the C-SCRM Program Management Office (PMO) to apply C-SCRM practices and capabilities needed to assess, respond to, and monitor cyber supply chain risk arising from pursuit of [Mission and Business Process]'s core objectives
- integrate C-SCRM activities into applicable activities to support [Organization]'s objective to manage cyber supply chain risk
- assign and dedicate resources responsible for coordinating C-SCRM activities within [Mission and Business Process]
- identify [Mission and Business Process]'s critical suppliers and assess level of risk exposure that arises as a result of that relationship
- implement risk response efforts to reduce exposure to cyber supply chain risk
- monitor [Mission and Business Process]'s ongoing exposure cyber supply chain risk profile and provide periodic reporting to identified [Organization] enterprise risk management and C-SCRM stakeholders

### 2.1.4. Roles & Responsibilities

*State those responsible for the C-SCRM policies, as well as its key contributors. Include the role and name of each individual or group, as well contact information where necessary (e.g., organizational affiliation, address, email address, and phone number).*

**Sample Level 1 Text**

- The C-SCRM Program Executive shall be responsible for:
    - leading the establishment, development, and oversight of the C-SCRM Program, in coordination and consultation with designated C-SCRM Leads;
    - establishing and serving as the Chair of the C-SCRM PMO. This Team will be comprised of the chair and the designated C-SCRM Leads and will be responsible for developing and coordinating C-SCRM strategy and implementation plans and actions, addressing C-SCRM-related issues, program reporting and oversight, and identifying and making program resource recommendations; and
    - escalating and/or reporting C-SCRM issues to Senior Officials, as may be appropriate.

- Each C-SCRM Security Officer shall be responsible for:
    - identify C-SCRM Leads (the Lead will be responsible for participating as a collaborative and core member of the C-SCRM PMO);
    - incorporate relevant C-SCRM functions into organization and position-level functions; and
    - implement and conform to C-SCRM Program requirements

**Sample Level 2 Text**

- C-SCRM Leads shall be responsible for:

        o   representing the interests and needs of C-SCRM PMO members; and

        o   leading and/or coordinating the development and execution of program or business-line C-SCRM plan(s). This shall include ensuring such plan(s) are appropriately aligned to and integrated with the enterprise-level C-SCRM plan.

- Mission and Business Process C-SCRM Staff shall be responsible for:
  - o Primary execution of C-SCRM activities (e.g., supplier or product assessments)
  - o Support mission and business-specific C-SCRM activities driven by non-C-SCRM staff

### 2.1.5. Definitions

*List the key definitions described within the policy, providing organizationally-specific context and examples where needed.*

**Sample Text (Applies to Level 1 and/or Level 2)**

- <u>Covered Articles:</u> Information technology, including cloud computing services of all types; Telecommunications equipment or telecommunications service; the processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program; all IoT/OT - (hardware, systems, devices, software, or services that include embedded or incidental information technology.

- <u>Cyber Supply Chain Risk Assessment:</u> Cyber Supply Chain Risk Assessment is a systematic examination of cyber supply chain risks, likelihoods of their occurrence, and potential impacts.

- <u>Risk Owner:</u> A person or entity with the accountability and authority to manage a risk.

### 2.1.6. Revision & Maintenance

*Define the required frequency for the C-SCRM policy. Maintain a table of revisions to enforce version control. C-SCRM policies are living documents that must be updated and communicated to all appropriate individuals (e.g., staff, contractors, and suppliers).*

**Sample Text (Applies to Level 1 and/or Level 2)**

[Organization's] C-SCRM policy must be reviewed at a minimum on an annual basis since changes to laws, policies, standards, guidelines, and controls are dynamic and evolving. Additional criteria that may trigger interim revisions include:

- change of policies that impact the C-SCRM policy;
- significant C-SCRM events;
- introduction of new technologies;
- discovery of new vulnerabilities;

7916　　　• operational or environmental changes;
7917　　　• shortcomings in the C-SCRM policy;
7918　　　• change of scope; and
7919　　　• other organization-specific criteria.

7920

7921　**Sample Version Management Table**

| Version Number | Date | Description of Change/Revision | Section/Pages Affected | Changes made by Name/Title/Organization |
|---|---|---|---|---|
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

7922

7923 **3. C-SCRM PLAN**
7924

7925 The C-SCRM plan is developed at Tier 3 and is implementation specific, providing policy
7926 implementation, requirements, constraints, and implications. It can either be stand-alone or
7927 components may be incorporated into system security and privacy plans. The C-SCRM plan
7928 addresses managing, implementation, and monitoring of C-SCRM controls and the
7929 development/sustainment of systems across the SDLC to support mission and business functions.
7930 The C-SCRM Plan applies to High and Moderate Impact systems per [FIPS 199].

7931 Given cyber supply chains can differ significantly across and within organizations, C-SCRM
7932 plans should be tailored to the individual program, organizational, and operational contexts.
7933 Tailored C-SCRM plans provide the basis for determining whether a technology, service, system
7934 component, or system is fit for purpose, and as such, the controls need to be tailored accordingly.
7935 Tailored C-SCRM plans help organizations focus their resources on the most critical mission and
7936 business functions based on mission and business requirements and their risk environment.

7937 The following C-SCRM Plan template is provided only as an example. Organizations have the
7938 flexibility to develop and implement various approaches for the development and presentation of
7939 the C-SCRM plan. Organizations can leverage automated tools to ensure all relevant sections of
7940 the C-SCRM plan are captured. Automated tools can help document C-SCRM plan information
7941 such as component inventories, individuals filling roles, security control implementation
7942 information, system diagrams, supply chain component criticality, and interdependencies.

7943 **3.1. C-SCRM Plan Template**
7944

7945 **3.1.1. System Name & Identifier**
7946

7947 *Designate a unique identifier and/or name for the system. Include any applicable historical*
7948 *names and relevant Tier 1 and Tier 2 document titles.*

7949 **Sample Text**

7950 This C-SCRM Plan provides an overview of the security requirements for the [SYSTEM
7951 NAME] [UNIQUE IDENTIFIER] and describes the cyber supply chain controls in place or
7952 planned for implementation to provide fit for purpose C-SCRM controls appropriate for the
7953 information to be transmitted, processed or stored by the system.

7954 The security safeguards implemented for the [UNIQUE IDENTIFIER] meet the requirements set
7955 forth in the organization's C-SCRM strategy and policy guidance.

7956 **3.1.2. System Description**
7957

7958 *Describe the function, purpose, and scope of the system and include a description of the*
7959 *information processed. Provide a general description of the system's approach to managing*
7960 *supply chain risks associated with the research and development, design, manufacturing,*

*acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services.*

*Ensure the C-SCRM plan describes the system in the context of the organization's supply chain risk tolerance, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, and a description of and justification for supply chain risk mitigation measures taken. Descriptions must be consistent with the high-level mission/business function of the system, the authorization boundary of the system, overall system architecture, including any supporting systems and relationships, how the system supports organizational missions, and the system environment (e.g., standalone, managed/enterprise, custom/specialized security-limited functionality, cloud) established in Level 1 and 2.*

**Sample Text**

The [Organization's] document management system (DMS) serves to provide dynamic information repositories, file hierarchies, and collaboration functionality to streamline internal team communication and coordination. The data managed within the system contains personally identifiable information (PII). The DMS is a commercial off-the-shelf (COTS) solution that was purchased directly from a verified supplier [Insert Supplier's name] within the United States. It has been functionally configured to meet the organization's needs; no third-party code libraries are utilized to deploy or maintain the system. It is hosted within the management layer of the organization's primary virtual private cloud provider.

The DMS is a Category 1 system, mandating a recovery time objective (RTO) of one hour in the event of downtime. The organization maintains a disaster recovery environment with a second private cloud provider that the organization can cutover to if the Category 1 RTO is not likely to be met on the primary platform.

### 3.1.3. System Information Type & Categorization

*The following tables specify the information types that are processed, stored, or transmitted by the system and/or its in-boundary cyber supply chain. Organizations utilize NIST [SP 800-60 v2], [NARA CUI], or other organization-specific information types to identify information types and provisional impact levels. Using guidance with regard to the categorization of federal information and systems in [FIPS 199], the organization determines the security impact levels for each information type. For each security objective (i.e., confidentiality, integrity, availability), provide the impact level (i.e., low, moderate, high).*

7993  **Sample Text**

| Information Type | Security Objectives | | |
|---|---|---|---|
| | Confidentiality (Low, Moderate, High) | Integrity (Low, Moderate, High) | Availability (Low, Moderate, High) |
| | | | |
| | | | |
| | | | |

7994  Based on the table above, indicate the high-water mark for each of the security impacts (i.e., low,
7995  moderate, high). Determine the overall system categorization.

| Security Objective | Security Impact Level |
|---|---|
| Confidentiality | ☐ Low ☐ Moderate ☐ High |
| Integrity | ☐ Low ☐ Moderate ☐ High |
| Availability | ☐ Low ☐ Moderate ☐ High |
| **Overall System Security Categorization** | ☐ **Low** ☐ **Moderate** ☐ **High** |

7996

7997  **3.1.4.  System Operational Status**
7998
7999  **Sample Text**
8000
8001  *Indicate the operational status of the system. If more than one status is selected, list which part*
8002  *of the system is covered under each status*

| System Status | | |
|---|---|---|
| ☐ | Operational | The system is currently operating and is in production. |
| ☐ | Under Development | The system is being designed, developed, or implemented |
| ☐ | Major Modification | The system is undergoing a major change, development, or transition. |
| ☐ | Disposition | The system is no longer operational. |

8003
8004
8005   **3.1.5.  System/Network Diagrams, Inventory, & Lifecycle Activities**

8006   *Include a current and detailed system and network diagram including a system component*
8007   *inventory or reference to where diagrams and inventory information can be found.*

8008   *Contextualize the above components against the system's SDLC to ensure activities are mapped*
8009   *and tracked. This ensures full coverage of C-SCRM activities since these activities may require*
8010   *repeating and reintegrating (using spiral or agile techniques) throughout the lifecycle. C-SCRM*
8011   *plan activities are required from concept, all the way through development, production,*
8012   *utilization, support, and retirement steps.*

8013   **Sample Text**

8014   [SYSTEM NAME] components may include:

8015   • Component description
8016   • Version number
8017   • License number
8018   • License holder
8019   • License type (e.g., single user, public license, freeware)
8020   • Barcode/property number
8021   • Hostname (i.e., the name used to identify the component on a network)
8022   • Component type (e.g., server, router, workstation, switch)
8023   • Manufacturer
8024   • Model
8025   • Serial number
8026   • Component revision number (e.g., firmware version)
8027   • Physical location: (include specific rack location for components in computer/server
8028     rooms)
8029   • Vendor name(s)

8030

8031   **3.1.6.  Information Exchange & System Connections**

8032   *List any information exchange agreements (e.g., Interconnection Security Agreements (ISA),*
8033   *Memoranda of Understanding (MOU), Memoranda of Agreement (MOA)) between the system*
8034   *and another system, date of the agreement, security authorization status of the other system(s),*
8035   *and the name of the authorizing official, provide a description of the connection, and include any*
8036   *diagrams showing the flow of any information exchange.*

8037   **Sample Text**

| Agreement Date | Name of System | Organization | Type of Connection or Information Exchange Method | FIPS 199 Categorization | Authorization Status | Authorization Official Name and Title |
|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### 3.1.7. Security Control Details

*Document C-SCRM controls to ensure the plan addresses requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes. Consider relevant topic areas such as assessments, standard operating procedures, responsibilities, software, hardware, product, service, and DevSecOps considerations.*

*For each control, provide a thorough description of how the security controls in the applicable baseline are implemented. Include any relevant artifacts for control implementation. Incorporate any control-tailoring justification, as needed. Reference applicable Level 1 and/or Level 2 C-SCRM policies that provide inherited controls where applicable. There may be multiple Level 1 policies that come from the CIO, CAO, or PMO.*

**Sample Text**

**SR-6 SUPPLIER ASSESSMENTS AND REVIEWS**

Implementation: As a part of a comprehensive, defense-in-breadth information security strategy, the organization established a C-SCRM program to address the management of cyber supply chain risks. The C-SCRM PMO is responsible for conducting cyber supply chain risk assessment (SCRA) for business partners seeking to integrate with [SYSTEM NAME] in accordance with enterprise-wide C-SCRM Level 2 policy requirements. C-SCRM training and awareness materials must also be provided for all individuals prior to receiving access to [SYSTEM NAME].

Control Enhancements: Control enhancements 2, 7 and 8 from NIST 800-161 are applicable.

(2) SUPPLIER REVIEWS
Implementation: C-SCRM PMO provides supplier reviews to business partners in the form of SCRAs before entering into a contractual agreement to acquire information systems, components, or services in relation to [SYSTEM NAME]. The Level 1 strategy and Level 2 policy documents place SCRA requirements on business partners seeking to acquire IT systems,

8073  components, and/or services. The SCRA provides a step-by-step guide for business partners to
8074  follow in preparing for an assessment of suppliers by the C-SCRM PMO.
8075
8076  (7) ASSESSMENT PRIOR TO SELECTION/ACCEPTANCE/UPDATE
8077  Implementation: The Level 2 policy defines what [SYSTEM NAME] integration activities
8078  require an SCRA. The process and requirements are defined in the SCRA Standard Operating
8079  Procedure.
8080
8081  (8) USE OF ALL-SOURCE INTELLIGENCE
8082  Implementation: The C-SCRM PMO utilizes all-source intelligence when conducting supply
8083  chain risk assessments for [SYSTEM NAME].
8084
8085  **3.1.8.  Role Identification**

8086  *Identify the role, name, department/division, primary and alternate phone number, email address*
8087  *of key cyber supply chain personnel or designate contacts (e.g., vendor contacts, acquisitions*
8088  *subject matter experts (SME), engineering leads, business partners, service providers), with role,*
8089  *name, address, primary and alternate phone numbers, and email address.*

8090  **Sample Text**

| Role | Name | Department/ Division | Primary Phone Number | Alternate Phone Number | Email Address |
|---|---|---|---|---|---|
| Vendor Contact | | | | | |
| Acquisitions SME | | | | | |
| Engineering Lead | | | | | |
| Business Partner | | | | | |
| Service Provider | | | | | |

8091

8092  **3.1.9.  Contingencies & Emergencies**
8093
8094  *In the event of contingency or emergency operations, organizations may need to bypass normal*
8095  *acquisition processes to allow for mission continuity. Contracting activities that are not vetted*
8096  *using approved C-SCRM plan processes introduce operational risks to the organization.*
8097  *Where appropriate, describe abbreviated acquisition procedures to follow during contingencies*
8098  *and emergencies, such as the contact information for C-SCRM, acquisitions, and legal subject*
8099  *matter experts who can provide advice absent a formal tasking and approval chain of command.*
8100
8101  **Sample Text**

8102    In the event of an emergency where equipment is urgently needed, the C-SCRM PMO will offer
8103    its assistance through C-SCRM Subject Matter Experts (SMEs) to provide help in the absence of
8104    the formal tasking and chain of command approval. The CIO has the authority to provide such
8105    waivers to bypass normal procedures. The current contact information for C-SCRM SMEs is
8106    provided below:

8107    - C-SCRM SME POC
8108        Name
8109        Email
8110        Phone
8111    - Acquisitions SME POC
8112        Name
8113        Email
8114        Phone
8115    - Legal SME POC
8116        Name
8117        Email
8118        Phone
8119

**8120    3.1.10. Related Laws, Regulations, & Policies**

8121    *List any applicable laws, executive orders, directives, policies, and regulations that are*
8122    *applicable to the system. For Level 3, include applicable Level 1 C-SCRM Strategy and*
8123    *Implementation Plans and Level 2 C-SCRM Policy titles.*

**8124    Sample Text**

8125    The organization shall ensure that C-SCRM plan controls are consistent with applicable statutory
8126    authority, including the Federal Information Security Modernization Act (FISMA); with
8127    regulatory requirements and external guidance, including Office of Management and Budget
8128    (OMB) policy and Federal Information Processing Standards (FIPS) publications promulgated
8129    by the National Institute of Standards and Technology (NIST); and with internal C-SCRM
8130    policies and strategy documents.
8131
8132    The following references apply:

8133    - Committee on National Security Systems. CNSSD No. 505. *(U) Supply Chain Risk*
8134        *Management (SCRM)*
8135    - NIST SP 800-53 Revisions 5 *Security and Privacy Controls for Information Systems and*
8136        *Organizations*
8137    - NIST SP 800-161 Revision 1 *Supply Chain Risk Management Practices for Information*
8138        *Systems and Organizations*
8139    - OMB Circular A-130 *Managing Information as a Strategic Resource*
8140    - Federal Acquisition Supply Chain Security Act of 2018
8141

8142    **3.1.11. Revision & Maintenance**

8143    *Include a table identifying the date of the change, a description of the modification, and the*
8144    *name of the individual who made the change. At a minimum, review and update Level 3 C-SCRM*
8145    *plans at life cycle milestones, gate reviews, and significant contracting activities, and verify for*
8146    *compliance with upper tier plans as appropriate. Ensure the plan adapts to shifting impacts of*
8147    *exogenous factors, such as threats, organizational, and environmental changes.*

8148    **Sample Text**

| Version Number | Date | Description of Change/Revision | Section/Pages Affected | Changes made by Name/Title/Organization |
|---|---|---|---|---|
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
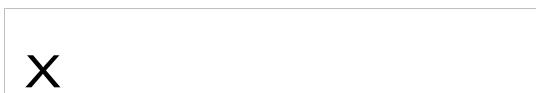
8149

8150    **3.1.12. C-SCRM Plan Approval**

8151    *Include a signature (either electronic or handwritten) and date when the system security plan is*
8152    *reviewed and approved.*

8153    **Sample Text**

8154         Authorizing Official:

         X
         _____
            Name
            Date

8155
8156    **3.1.13. Acronym List**

8157    *Include and detail any acronyms utilized in the C-SCRM plan.*

8158    **Sample Text**

| Acronym | Detail |
|---|---|
| AO | Authorizing Official |
| C-SCRM | Cyber Supply Chain Risk Management |
| SDLC | System Development Life Cycle |

8159

8160 **3.1.14. Attachments**
8161

8162 *Attach any relevant artifacts that can be included to support the C-SCRM plan.*
8163
8164 **Sample Text**
8165
8166 • Contractual agreements
8167 • Contractors' or suppliers' C-SCRM plans

8168

8169  **4.  CYBER SUPPLY CHAIN RISK ASSESSMENT**
8170
8171  The Cyber Supply Chain Risk Assessment (C-SCRA) guides the review of any third-party
8172  product, service, or supplier[41] that could present a cyber supply chain risk to a procurer. The
8173  objective of the C-SCRA template is to provide a toolbox of questions that an acquirer can
8174  choose to use or not use depending on the controls selected. Typically executed by C-SCRM
8175  PMOs at the operational level (Level 3), the C-SCRA takes into account available public and
8176  private information to perform a holistic assessment, including known cyber supply chain risks,
8177  likelihoods of their occurrence, and potential impacts to an organization and its information and
8178  systems. As organizations may be inundated with C-SCRAs, and suppliers inundated with C-
8179  SCRA requests, the organization should evaluate the relative priority of its C-SCRAs as an
8180  influencing factor on the rigor of the C-SCRA.

8181  As with the other featured templates, the below C-SCRA is provided only as an example.
8182  Organizations must tailor the below content to align with their Level 1 and 2 risk postures. The
8183  execution of C-SCRAs is perhaps the most visible and time-consuming component of C-SCRM
8184  operations and must therefore be designed for efficient execution at scale with dedicated support
8185  resources, templated workflows, and automation wherever possible.

8186

8187  **4.1.C  SCRM Template**
8188

8189  **4.1.1.  Authority & Compliance**
8190
8191  *List of the laws, executive orders, directives, regulations, policies, standards, and guidelines that*
8192  *govern C-SCRA execution.*
8193
8194  **Sample Text**

8195  - Legislation
8196       - Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
8197         Technology Act (SECURE) Technology of 2018
8198  - Policies
8199       - [Organization Name] C-SCRA Standard Operating Procedures
8200       - [Organization Name] C-SCRA Risk Assessment Factors
8201       - [Organization Name] C-SCRA Criticality Assessment Criteria
8202  - Guidelines
8203       - NIST 800-53 Revision 5: PM-30, RA-3, SA-15, SR-5
8204       - NIST 800-37 Revision 2
8205       - NIST 800-161 Revision 1: Appendix C
8206       - ISO 28001:2007
8207

---

[41] A supplier may also refer to a source, as defined in the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure
Technology Act (SECURE) Technology of 2018

### 4.1.2. Description

*Describe the purpose and scope of the C-SCRA template, referencing the organizational commitment to C-SCRM and mandate to perform C-SCRAs as an extension of that commitment. Outline the templates relationship to organizational risk management principles, frameworks, practices. This may include providing an overview of the organization's C-SCRA processes, standard operating procedures, and/or criticality designations that govern usage of this template.*

*Reinforce the business case for executing C-SCRAs by highlighting the benefits of reducing expected loss from adverse cyber supply chain events, as well as the C-SCRM PMOs role in executing these assessments efficiently at scale.*

*Provide an overview of the organizational boundaries, systems, and services within the scope of the C-SCRAs.*

*List the contact information and other resources that readers may access in order to further engage with the C-SCRA process.*

**Sample Text**

This C-SCRA is intended to evaluate risks, in a fair and consistent manner, posed to the [Organization] via third parties that hold the potential for harm or compromise arising as a result of cybersecurity risks. Cyber supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain as well as the exposures, threats, and vulnerabilities to the supply chain and its suppliers.

The C-SCRA template provides tactical guidelines for the [Organization's C-SCRM PMO] to review cyber supply chain risks and ensure that C-SCRAs are appropriately carried out in line with organizational mandates efficiently and effectively.

Requestors seeking to introduce third party products, services, or suppliers into organizational boundaries should familiarize themselves with the following template. This will ensure that requestors can provide the requisite information to the C-SCRM PMO to ensure timely execution of C-SCRAs and are otherwise aligned with adhering to the steps of the C-SCRA.

The C-SCRA process contains five primary steps, as outlined in the below template:[42]
1. Information Gathering & Scoping Analysis
2. Threat Analysis
3. Vulnerability Analysis
4. Impact Analysis
5. Risk Response Analysis

---

[42] See Appendix D's "Assess" section for the methodological principles and guidance that underpin these steps.

8251 To learn more about the C-SCRA process and/or submit an assessment request to the C-SCRM
8252 PMO, please go to [Organizational intranet page] or contact [C-SCRM PMO email].
8253
8254 **4.1.3. Information Gathering & Scoping Analysis**
8255
8256 *Define the purpose and objectives for the requested C-SCRA, outlining the key information*
8257 *required to appropriately define the system, operations, supporting architecture, and*
8258 *boundaries. Provide key questions to requestors to facilitate collection and analysis of this*
8259 *information. The C-SCRM PMO will then use this information as a baseline for subsequent*
8260 *analyses and data requests.*
8261
8262 **Sample Text**

| Supply Chain Risk Management Assessment Scoping Questionnaire | | |
|---|---|---|
| Section 1: Request Overview | Provide Response: | Response Provided by: |
| Requestor Name | | Acquirer |
| C-SCRA Purpose and Objective | | Acquirer |
| System Description | | Acquirer |
| Architecture Overview | | Acquirer |
| Boundary Definition | | Acquirer |
| Date of Assessment | | Acquirer |
| Assessor Name | | Acquirer |
| Section 2: Product/Service Internal Risk Overview | | |
| What is the suppliers market share for this particular product/service | | Acquirer |
| What % of this supplier's sales of this product/service does your organization consume? | | Acquirer |
| How widely used will the product or service be in your organization? | | Acquirer |
| Is the product/service manufactured in a geographic location that is considered an area of geopolitical risk for your organization based on it's primary area of operation (e.g., in the United States). | | Acquirer |
| Would switching to an alternative supplier for this product or service constitute significant cost or effort for your organization? | | Acquirer |
| Does your organization have an existing relationship with another supplier for this product/service? | | Acquirer |
| How confident is your organization that they will be able to obtain quality | | Acquirer |

233

| | | |
|---|---|---|
| products/services regardless of major supply chain disruptions, both manmade and natural | | |
| Does your organization maintain a reserve of this product/service? | | Acquirer |
| Is the product/service fit for purpose? (i.e., capable of meeting is objectives or service levels) | | Acquirer |
| Does the product/service perform an essential security function? Please describe | | Acquirer |
| Does the product/service have root access to IT networks, OT systems or sensitive platforms? | | Acquirer |
| Can compromise of the product/service lead to system failure or severe degradation? | | Acquirer |
| Is there a known independent reliable mitigation for compromise leading to system failure or severe degradation? | | Acquirer |
| Does the product/service connect to a platform that is provided by your organization to customers? | | Acquirer |
| Does the product/service transmit, generate, maintain, or process high value data? | | Acquirer |
| Does the product/service have access to systems that transmit, generate, maintain or process high value data (e.g., PII, PHI, PCI) | | Acquirer |
| Does the supplier require physical access to the companies facilities as a result of its provision of the product/service? | | Acquirer |
| Based on holistic consideration of the above responses, how critical is this product/service to your organization (e.g., Critical, High, Moderate, Low) | | Acquirer |
| Section 2: Supplier Overview | | |
| Have you identified the supplier's key suppliers? | | Supplier |
| Did you verify the supplier ownership, both foreign and domestic? | | Supplier |
| If the supplier uses distributors, did you investigate them for potential threats? | | Supplier |
| Is the supplier located in the United States? | | Supplier |
| Has the supplier declared where replacement components will be purchased from? | | Supplier |
| Have all of the suppliers', subcontractors', and suppliers' owners and locations been validated? | | Supplier |

| | | |
|---|---|---|
| Does the supplier vet suppliers for threat scenarios? | | Supplier |
| Does the supplier have documents which track part numbers to manufacturers? | | Supplier |
| Can the supplier provide a list of who they procure COTS software from? | | Supplier |
| Does the supplier have counterfeit controls in place? | | Supplier |
| Does the supplier safeguard key program information that may be exposed through interactions with suppliers? | | Supplier |
| Does the supplier perform reviews, inspections, and have safeguards to detect/avoid counterfeit equipment, tampered hardware/software (HW/SW), vulnerable HW/SW, and/or operations security leaks leaks? | | Supplier |
| Does the supplier use industry standards baselines (e.g., CIS, NES) when purchasing software? | | Supplier |
| Does the supplier comply with regulatory and legislation mandates? | | Supplier |
| Does the supplier have procedures for secure maintenance and upgrades following deployment? | | Supplier |
| Section 3: Policies & Procedures | | |
| Does the supplier have definitive policies and procedures that help minimize supply chain risk, including subsidiary sourcing needs? | | Supplier |
| Does the supplier define and manage system criticality and capability? | | Supplier |
| Does everyone associated with the procurement (e.g., supplier, C-SCRM PMO) understand the threats and risks in the subject supply chain? | | Supplier |
| Are all engaged personnel US citizens? | | Supplier |
| Does the supplier have "insider threat" controls in place? | | Supplier |
| Does the supplier verify and monitor all personnel that interact with the subject product, system, or service to know if they pose a threat? | | Supplier |

| | | |
|---|---|---|
| Does the supplier use, record, and track risk mitigation activities throughout the life cycle of the product, system, or service? | | Supplier |
| Have all of the supplier's personnel signed non-disclosure agreements? | | Supplier |
| Does the supplier allow its personnel or suppliers to access environments remotely (i.e. from an out of boundary)? | | Supplier |
| **Section 4: Logistics (if applicable)** | | |
| Does the supplier have documented tracking and version controls in place? | | Supplier |
| Does the supplier analyze events (environmental or man-made) that could interrupt their supply chain? | | Supplier |
| Are the supplier's completed parts controlled, so they are never left unattended or exposed to tampering? | | Supplier |
| Are the supplier's completed parts locked up? | | Supplier |
| Does the C-SCRM PMO have a process that ensures integrity when ordering inventory from the supplier? | | Supplier |
| Does the C-SCRM PMO periodically inspect the supplier's inventory for exposure or tampering? | | Supplier |
| Does the C-SCRM PMO have secure material destruction procedures for unused and scrap parts procured from the supplier? | | Supplier |
| Is there a documented chain of custody for the deployment of products and systems? | | Supplier |
| **Section 5: Software Design & Development (if applicable)** | | |
| Is the C-SCRM PMO familiar with all the suppliers that will work on the design of the product/system? | | Supplier and Manufacturer |
| Does the supplier align its SDLC to a secure software development standard (e.g., Microsoft Security Development Lifecycle) | | Supplier and Manufacturer |
| Does the supplier perform all development onshore? | | Supplier and Manufacturer |
| Do only United States citizens have access to development environments? | | Supplier and Manufacturer |
| Does the supplier provide cybersecurity training to its developers? | | Supplier and Manufacturer |
| Does the supplier use trusted software development tools? | | Supplier and Manufacturer |

| | | |
|---|---|---|
| Is the supplier using trusted information assurance controls to safeguard the development environment (e.g., secure network configurations, strict access controls, dynamic/static vulnerability management tools, penetration testing)? | | Supplier and Manufacturer |
| Does the supplier validate open source software prior to use? | | Supplier and Manufacturer |
| Are the supplier's software compilers continuously monitored? | | Supplier and Manufacturer |
| Does the supplier have codified software test and configuration standards? | | Supplier and Manufacturer |
| **Section 6: Product/Service Specific Security (if applicable, one questionnaire per product/service)** | | |
| Product / Service Name | | Manufacturer |
| Product Type (s) (Hardware, Software, Service) | | Manufacturer |
| Product / Service Description | | Manufacturer |
| Part Number (if applicable) | | Manufacturer |
| Does the manufacturer implement formal organizational roles and governance responsible for the implementation and oversight of Secure Engineering across the development or manufacturing process for product offerings? | | Manufacturer |
| Does the manufacturer have processes for product integrity conform to any of the following standards (e.g., ISO 27036, SAE AS6171, etc.)? | | Manufacturer |
| Is the product Federal Information Processing Standards (FIPS) compliant? If yes, please provide the FIPS level | | Manufacturer |
| Does the manufacturer document and communicate security control requirements for your hardware, software, or solution offering? | | Manufacturer |
| Has the manufacturer received fines or sanctions from any governmental entity or regulatory body in the past year related to the delivery of the product or service? If yes, please describe. | | Manufacturer |
| Has the manufacturer experienced litigation claims over the past year related to the delivery of the product or service? If yes, please describe | | Manufacturer |

| | | |
|---|---|---|
| Does the manufacturer provide a bill of materials (BOM) for the products or service, and components which includes all logic-bearing (e.g., readable/writable/programmable) hardware, firmware, and software? | | Manufacturer |
| For hardware components included in the product or service offering, does the supplier only buy from original equipment manufacturers or licensed resellers? | | Supplier |
| Does the manufacturer have a policy or process to ensure that none of your suppliers or third-party components are on any banned list? | | Manufacturer |
| How does the manufacturer prevent malicious and/or counterfeit IP components within their product offering or solution? | | Manufacturer |
| Does the manufacturer manage the integrity of IP for its product or service offering? | | Manufacturer |
| How does the manufacturer assess, prioritize, and remediate reported product or service vulnerabilities? | | Manufacturer |
| How does the manufacturer ensure that product or service vulnerabilities are remediated in a timely period, reducing the window of opportunity for attackers? | | Manufacturer |
| Does the manufacturer maintain and manage a Product Security Incident Reporting and Response program (PSRT)? | | Manufacturer |
| What is the manufacturer's process to ensure customers and external entities (such as government agencies) are notified of an incident when their product or service is impacted? | | Manufacturer |

8263
8264 **4.1.4. Threat Analysis**
8265
8266 *Define threat analysis as well as the criteria that will be utilized to assess the threat of the*
8267 *product, service, or supplier being assessed. Include a rubric with categorical definitions to*
8268 *encourage transparency behind assessment results.*
8269
8270 **Sample Text**

8271 The C-SCRA threat analysis evaluates and characterizes the level of threat to the integrity,
8272 trustworthiness, and authenticity of the product, service, or supplier as described below.

8273   This analysis is based on a threat actor's capability and intent to compromise or exploit the
8274   product, service, or supplier being introduced into the cyber supply chain. Following completion
8275   of the analysis, one of the following threat levels is assigned:

- 8276   **Critical:** Information indicates adversaries are engaged in subversion, exploitation, or
  8277   sabotage of the product, service, or supplier.
- 8278   **High:** Information indicates adversaries have established an overt or clandestine
  8279   relationship with the product, service, or supplier, with the capability and intent to engage
  8280   in subversion, exploitation or sabotage of the supply chain; however, there are no known
  8281   indications of subversion, exploitation, or sabotage.
- 8282   **Moderate:** Information indicates adversaries have the capability but NOT the intent to
  8283   engage in subversion, exploitation or sabotage of the product, service, or supplier.
  8284   Conversely, they may have the intent but NOT the capability.
- 8285   **Low:** Information indicates adversaries have neither the capability nor the intent to
  8286   engage in subversion, exploitation, or sabotage of the product, service, or supplier.

8287   To appropriately assign the above threat analysis designation, C-SCRM PMOs and requestors
8288   should leverage the Information Gathering & Scoping questionnaire to coordinate collection of
8289   information related to the product, service, or supplier's operational details, ownership structure,
8290   key management personnel, financial information, business ventures, government restrictions,
8291   and potential threats. Additional investigations should be performed against the aforementioned
8292   topics if red flags are observed during initial data collection.
8293
8294   **4.1.5. Vulnerability Analysis**
8295
8296   *Define vulnerability analysis as well as the criteria that will be utilized to assess the*
8297   *vulnerability of the product, service, or supplier being assessed. Include a rubric with*
8298   *categorical definitions to encourage transparency behind assessment results.*
8299

8300   **Sample Text**

8301   The C-SCRA vulnerability analysis evaluates and then characterizes the vulnerability of the
8302   product, service, or supplier throughout its lifecycle and/or engagement. The analysis includes an
8303   assessment of the ease of exploitation by a threat actor with moderate capabilities.
8304   This analysis is based on a threat actor's capability and intent to compromise or exploit the
8305   product, service, or supplier being introduced into the cyber supply chain. Following completion
8306   of the analysis, one of the following threat levels is assigned:

- 8307   **Critical:** The product, service, or supplier contains vulnerabilities that are wholly
  8308   exposed (physically or logically) and are easily exploitable.
- 8309   **High:** The product, service, or supplier contains vulnerabilities that are highly exposed
  8310   and are reasonably exploitable.
- 8311   **Moderate:** The product, service, or supplier contains vulnerabilities that are moderately
  8312   exposed and would be difficult to exploit.
- 8313   **Low:** The product, service, or supplier is not exposed and would be unlikely to be
  8314   exploited.

8315 To appropriately assign the above vulnerability analysis designation, C-SCRM PMOs and
8316 requestors should coordinate to collect information related to the product, service, or supplier's
8317 operational details, exploitability, service details, attributes of known vulnerabilities, and
8318 mitigation techniques.
8319
8320 **4.1.6. Impact Analysis**
8321
8322 *Define impact analysis as well as the criteria that will be utilized to assess the criticality of the*
8323 *product, service, or supplier being assessed. Include a rubric with categorical definitions to*
8324 *encourage transparency behind assessment results.*
8325

8326 **Sample Text**

8327 The C-SCRA impact analysis evaluates and then characterizes the impact of the product, service,
8328 or supplier throughout its lifecycle and/or engagement. The analysis includes an end-to-end
8329 functional review to identify critical functions and components based on an assessment of the
8330 potential harm caused by the probable loss, damage, or compromise of a product, material, or
8331 service to an [Organization's] operations or mission.
8332 Following completion of the analysis, one of the following impact levels is assigned:

- **Critical:** The product, service, or supplier's failure to perform as designed would result
  8334 in a total organizational failure or a significant and/or unacceptable level of degradation
  8335 of operations that could only be recovered with exceptional time and resources.
- **High:** The product, service, or supplier's failure to perform as designed would result in
  8337 severe organizational failure or a significant and/or unacceptable level of degradation of
  8338 operations that could only be recovered with significant time and resources.
- **Moderate:** The product, service, or supplier's failure to perform as designed would result
  8340 in serious organizational failure that could readily and quickly managed with no long-
  8341 term consequences.
- **Low:** The product, service, or supplier's failure to perform as designed would result in
  8343 very little adverse effects on the organization that could readily and quickly managed
  8344 with no long-term consequences.

8345 To appropriately assign the above impact analysis designation, C-SCRM PMOs and requestors
8346 should coordinate to collect information related to [Organization's] critical functions and
8347 components, identification of the intended user environment for the product or service, and
8348 supplier information.
8349
8350 **4.1.7. Risk Response Analysis**
8351
8352 *Define risk analysis as well as the criteria that will be utilized to assess the scoring of the*
8353 *product or service being assessed. Include a rubric with categorical definitions to encourage*
8354 *transparency behind assessment results.*
8355
8356 **Sample Text**

8357    The C-SCRA risk score reflects a combined judgement based on likelihood and impact analyses.
8358    The likelihood analysis is scored via a combination of the aforementioned threat and
8359    vulnerability analysis score, as outlined in the figure below.

| Likelihood Level | | | | | |
|---|---|---|---|---|---|
| | | **Vulnerability** | | | |
| | | Low | Moderate | High | Critical |
| **Threat** | Very Likely | Moderately Likely | Highly Likely | Very Likely | Very Likely |
| | Highly Likely | Moderately Likely | Highly Likely | Highly Likely | Very Likely |
| | Moderately Likely | Unlikely | Moderately Likely | Highly Likely | Highly Likely |
| | Unlikely | Unlikely | Unlikely | Moderately Likely | Moderately Likely |

8360
8361    The C-SCRA risk score is then aggregated based upon that likelihood score and the impact score.
8362    If multiple vulnerabilities are identified for a given product or service, each vulnerability shall be
8363    assigned a risk level based upon its likelihood and impact.

| Overall Risk Score | | | | | |
|---|---|---|---|---|---|
| | | **Impact** | | | |
| | | Low | Moderate | High | Critical |
| **Likelihood (threat and vulnerability)** | Very Likely | Moderate | High | Critical | Critical |
| | Highly Likely | Moderate | Moderate | High | Critical |
| | Moderately Likely | Low | Moderate | High | High |
| | Unlikely | Low | Low | Moderate | High |

8364
8365    The aforementioned risk analyses and scoring provide measures by which [Organization]
8366    determines whether or not to proceed with procurement of the product, service, or supplier.
8367    Decisions to proceed must weighed against the risk appetite and tolerance across the tiers of the
8368    organization, as well as the mitigation strategy that may be put in place to manage the risks as a
8369    result of procuring the product, service, or supplier.
8370

8371 **4.1.8. Roles & Responsibilities**
8372
8373 *State those responsible for the C-SCRA policies, as well as its key contributors. Include the role*
8374 *and name of each individual or group, as well contact information where necessary (e.g.,*
8375 *organizational affiliation, address, email address, and phone number).*
8376
8377 **Sample Text**

8378 • C-SCRM PMO shall:

8379      o maintaining C-SCRA policies, procedures, and scoring methodologies
8380      o performing C-SCRA standard operating procedures
8381      o liaising with requestors seeking to procure a product, service or supplier
8382      o reporting C-SCRA results to leadership to help inform organizational risk posture
8383

8384 • Each requestor shall:
8385      o complete C-SCRA request forms and provide all required information
8386      o address any information follow-up requests from the C-SCRM PMO resource
8387         completing the C-SCRA
8388      o adhering to any stipulations or mitigations mandated by the C-SCRM PMO
8389         following approval of a C-SCRA request.
8390

8391 **4.1.9. Definitions**
8392
8393 *List the key definitions described within the policy, providing organizationally-specific context*
8394 *and examples where needed.*
8395
8396 **Sample Text**

8397 • Procurement: Process of obtaining a system, product, or service.
8398

8399 **4.1.10. Revision & Maintenance**
8400
8401 *Define the required frequency for the C-SCRA template. Maintain a table of revisions to enforce*
8402 *version control. C-SCRA templates are living documents that must be updated and*
8403 *communicated to all appropriate individuals (e.g., staff, contractors, and suppliers).*
8404
8405 **Sample Text**
8406
8407 [Organization's] C-SCRA template must be reviewed at a minimum on an annual basis since
8408 changes to laws, policies, standards, guidelines, and controls are dynamic and evolving.
8409 Additional criteria that may trigger interim revisions include:

8410 • change of policies that impact the C-SCRA template;
8411 • significant C-SCRM events;
8412 • introduction of new technologies;
8413 • discovery of new vulnerabilities;

8414      •   operational or environmental changes
8415      •   shortcomings in the C-SCRA template;
8416      •   change of scope; and
8417      •   other organization-specific criteria.

8418

8419    **Sample Version Management Table**

| Version Number | Date | Description of Change/Revision | Section/Pages Affected | Changes made by Name/Title/Organization |
|---|---|---|---|---|
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

8420
8421

8422    **APPENDIX E: GLOSSARY**

| Term | Definition | Source |
|------|-----------|--------|
| Acceptable Risk | A level of residual risk to the organization's operations, assets, or individuals that falls within the defined risk appetite and risk tolerance thresholds set by the organization. | |
| Acquirer | Organization or entity that acquires or procures a product or service. | [ISO/IEC 15288] (adapted) |
| Acquisition | Includes all stages of the process of acquiring product or services, beginning with the process for determining the need for the product or services and ending with contract completion and closeout. | [NIST SP 800-64 Rev. 2] (adapted) |
| Agreement | Mutual acknowledgement of terms and conditions under which a working relationship is conducted or goods are transferred between parties. EXAMPLE: contract, memorandum, or agreement | |
| Authorization | Authorization to operate: The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems. | [NIST SP 800-53 Rev. 5] |
| Authorization Boundary | All components of an information system to be authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected | [NIST SP 800-53 Rev. 5] |
| Authorizing Official (AO) | A senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation. | [NIST SP 800-53 Rev. 5] |

| | | |
|---|---|---|
| Baseline | Hardware, software, databases, and relevant documentation for an information system at a given point in time. | [CNSSI No. 4009] |
| C-SCRM Control | A safeguard or countermeasures prescribed for the purpose of reducing or eliminating the likelihood and/or impact/consequences of a cyber supply chain risk. | |
| Cyber Supply Chain Risk | Cyber supply chain risk is the potential for harm or compromise that arises as a result of cybersecurity risks from suppliers, their supply chains, and their products or services. Cyber supply chain risks arise from threats that exploit vulnerabilities or exposures within products and services traversing the supply chain as well as threats exploiting vulnerabilities or exposures within the supply chain itself. | |
| Cyber Supply Chain Risk Assessment | Cyber Supply Chain Risk Assessment is a systematic examination of cyber supply chain risks, likelihoods of their occurrence, and potential impacts. | |
| Cyber Supply Chain Risk Management | A systematic process for managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the cyber supply chain risks presented by the supplier, the supplied products and services, or the supply chain. | |
| Defense-in-Breadth | A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle, including system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement. | [NIST SP 800-53 Rev. 5] |
| Defense-in-Depth | Information security strategy that integrates people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. | [NIST SP 800-53 Rev. 5] |
| Degradation | A decline in quality or performance; the process by which the decline is brought about. | |

| | | |
|---|---|---|
| Developer | A general term that includes developers or manufacturers of systems, system components, or system services; systems integrators; suppliers; and product resellers. Development of systems, components, or services can occur internally within organizations or through external entities | [NIST SP 800-53 Rev. 5] |
| Element | Supply chain element: Organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and/or disposal of systems and system components. | |
| Enhanced Overlay | An overlay that adds processes, controls, enhancements, and additional implementation guidance specific to the purpose of the overlay. | |
| Exposure | Extent to which an organization and/or stakeholder is subject to a risk | [ISO Guide 73:2009] (adapted) |
| External systems Service Provider | A provider of external system services to an organization through a variety of consumer-producer relationships, including joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. | [NIST SP 800-53 Rev. 5] |
| External System Service | A system service that is provided by an external service provider and for which the organization has no direct control over the implementation of required security and privacy controls or the assessment of control effectiveness. | [NIST SP 800-53 Rev. 5] |
| Fit for purpose | Fit for purpose is used informally to describe a process, configuration item, IT service, etc., that is capable of meeting its objectives or service levels. Being fit for purpose requires suitable design, implementation, control, and maintenance. | [ITIL Service Strategy] (adapted) |
| ICT/OT-related service providers | Any organization or individual providing services which may include authorized access to an ICT or OT system | |

| | | |
|---|---|---|
| Supplier | Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain, developers or manufacturers of systems, system components, or system services; systems integrators; suppliers; product resellers; and third-party partners. | [ISO/IEC 15288] (adapted); adapted from definition of "developer" from [NIST SP 800-53 Rev. 5] |
| Supply Chain | Supply chain: Linked set of resources and processes between and among multiple levels of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle. | [ISO 28001] (adapted) |
| System Integrator | An organization that customizes (e.g., combines, adds, optimizes) components, systems, and corresponding processes. The integrator function can also be performed by acquirer. | [NISTIR 7622] (adapted) |
| Cyber Supply Chain Compromise | Cyber supply chain incident (also known as compromise) is an occurrence within the supply chain whereby the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits is jeopardized. A cyber supply chain incident can occur anywhere during the life cycle of the system, product or service. | |
| Information and Communications Technology (ICT) | Encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information. | [ISO/IEC 2382] (adapted) |
| Information System | A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. | [NIST SP 800-53 Rev. 5] |
| Life cycle | Evolution of a system, product, service, project, or other human-made entity. | [ISO/IEC 15288] (adapted) |
| Likelihood | Chance of something happening | [ISO/IEC 27000:2018] |
| Organizational Users | An organizational employee or an individual the organization deemed to have similar status of an employee including, for example, contractor, guest researcher, or individual detailed from another organization. | [NIST SP 800-53 Rev. 4] (adapted) |

| | | |
|---|---|---|
| Overlay | A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. | [NIST SP 800-53 Rev. 5] |
| Pedigree | The validation of the internal composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software this includes the composition of open source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid. | |
| Provenance | The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. | [NIST SP 800-53 Rev. 5] |
| Risk | A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. | [NIST SP 800-39] |
| Residual Risk | Portion of risk remaining after controls/counterrmeasures measures have been applied. | [NIST SP 800-16] (adapted) |
| Risk Appetite | The types and amount of risk, on a broad level, it is willing to accept in its pursuit of value | [NISTIR 8286] |
| Risk Framing | The set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization's approach for managing risk | [NIST SP 800-39] |

| | | |
|---|---|---|
| Risk Management | The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes: establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time. | [NIST SP 800-53 Rev. 5] |
| Risk Mitigation | Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. | [NIST SP 800-53 Rev. 5] |
| Risk Response | Intentional and informed decision and actions to accept, avoid, mitigate, share, or transfer an identified risk | [NIST SP 800-53 Rev. 5] (adapted) |
| Risk Response Plan | A summary of potential consequence(s) of the successful exploitation of a specific vulnerability or vulnerabilities by a threat agent, as well as mitigating strategies and C-SCRM controls | |
| Risk Tolerance | the organization or stakeholders' readiness to bear the remaining risk after responding to or considering the risk in order to achieve its objectives | [NIST 8286] |
| Secondary market | An unofficial, unauthorized, or unintended distribution channel. | |
| Security Control | The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information. | [NIST SP 800-53 Rev. 5] |
| Supplier | Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain, developers or manufacturers of systems, system components, or system services; systems integrators; suppliers; product resellers; and third-party partners. | [ISO/IEC 15288] (adapted)] |

| | | |
|---|---|---|
| System | Combination of interacting elements organized to achieve one or more stated purposes.<br>*Note 1:* There are many types of systems. Examples include: general and special-purpose information systems; command, control, and communication systems; crypto modules; central processing unit and graphics processor boards; industrial control systems; flight control systems; weapons, targeting, and fire control systems; medical devices and treatment systems; financial, banking, and merchandising transaction systems; and social networking systems.<br>*Note 2:* The interacting elements in the definition of system include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities.<br>*Note 3:* System-of-systems is included in the definition of system. | [NIST SP 800-53 Rev. 5] (adapted) |
| System Component | A discrete identifiable information or operational technology asset that represents a building block of a system and may include hardware, software, and firmware. | |
| System Development Life Cycle (SDLC) | The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal. | [NIST SP 800-34 Rev. 1] (adapted) |
| System Integrator | Those organizations that provide customized services to the acquirer including for example, custom development, test, operations, and maintenance. | |
| System Assurance | The justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle. | [NDIA] |
| System Owner | System owner (or program manager): Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system. | [NIST SP 800-53 Rev. 5] |

| | | |
|---|---|---|
| Threat | Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. | [NIST SP 800-53 Rev. 5] |
| Threat Assessment/Analysis | Formal description and evaluation of threat to a system or organization. | [NIST SP 800-53 Rev. 5] (adapted) |
| Threat Event | An event or situation that has the potential for causing undesirable consequences or impact. | [NIST SP 800-30 Rev. 1] |
| Threat Event Outcome | The effect a threat acting upon a vulnerability has on the confidentiality, integrity, and/or availability of the organization's operations, assets, or individuals. | |
| Threat Scenario | A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time. | [NIST SP 800-30 Rev. 1] |
| Threat Source | The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. | [NIST SP 800-53 Rev. 5] |
| Trust | The confidence one element has in another, that the second element will behave as expected. | [Software Assurance in Acquisition: Mitigating Risks to the Enterprise] |
| Trustworthiness | The interdependent combination of attributes of a person, system, or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. The degree to which a system (including the technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. | [NIST SP 800-53 Rev. 5] (adapted) |
| Validation | confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been | [ISO 9000] |

fulfilled
Note: The requirements were met.

| | | |
|---|---|---|
| Verification | confirmation, through the provision of objective evidence, that specified requirements have been fulfilled<br>Note: The intended output is correct. | [CNSSI No. 4009], [ISO 9000] (adapted) |
| Visibility (also Transparency) | Amount of information that can be gathered about a supplier, product, or service and how far through the supply chain this information can be obtained | [ISO/IEC 27036-2] (adapted) |
| Vulnerability | Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. | [NIST SP 800-53 Rev. 5] |
| Vulnerability Assessment | Systematic examination of a system or product or supply chain element to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. | [NIST SP 800-53 Rev. 5] (adapted) |

8423
8424

8425

8426 **APPENDIX F: ACRONYMS**

| A&A | Assessment and Authorization |
|-----|------------------------------|
| AO | Authorizing Official |
| API | Application Programming Interface |
| APT | Advanced Persistent Threat |
| BIA | Business Impact Analysis |
| BYOD | Bring Your Own Device |
| CAC | Common Access Card |
| CAO | Chief Acquisition Officer |
| CEO | Chief Executive Officer |
| CFO | Chief Financial Officer |
| CIO | Chief Information Officer |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CISO | Chief Information Security Officer |
| CLO | Chief Legal Officer |
| COO | Chief Operating Officer |
| CPO | Chief Privacy Officer |
| CRO | Chief Risk Officer |
| CTO | Chief Technology Officer |
| CNSS | Committee on National Security Systems |
| CNSSI | Committee on National Security Systems Instruction |
| CONUS | Continental United States |
| COSO | Committee of Sponsoring Organizations of the Treadway Commission' |
| COTS | Commercial Off-The-Shelf |
| CRO | Chief Risk Officer |

| C-SCRM | Cyber Supply Chain Risk Management |
|--------|-------------------------------------|
| CSF | Cybersecurity Framework |
| CTO | Chief Technology Officer |
| CUI | Controlled Unclassified Information |
| CVE | Common Vulnerability Enumeration |
| CVSS | Common Vulnerability Scoring System |
| DHS | Department of Homeland Security |
| DMEA | Defense Microelectronics Activity |
| DoD | Department of Defense |
| DODI | Department of Defense Instruction |
| ERM | Enterprise Risk Management |
| ERP | Enterprise Resource Planning |
| FAR | Federal Acquisition Regulation |
| FARM | Frame, Assess, Respond, Monitor |
| FASC | Federal Acquisition Security Council |
| FASCA | Federal Acquisition Supply Chain Security Act |
| FBI | Federal Bureau of Investigation |
| FedRAMP | Federal Risk and Authorization Program |
| FIPS | Federal Information Processing Standards |
| FISMA | Federal Information Security Management Act |
| FITARA | Federal Information Technology Acquisition Reform Act |
| FOCI | Foreign Ownership, Control or Influence |
| FSP | Financial Services Cybersecurity Framework Profile |
| GAO | Government Accountability Office |
| GIDEP | Government-Industry Data Exchange Program |

| GOTS | Government Off-The-Shelf |
|---|---|
| GPS | Global Positioning System |
| HR | Human Resources |
| IA | Information Assurance |
| ICT | Information and Communication Technology |
| ICT/OT | Information, communications, and operational technology |
| IDE | Integrated Development Environment |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IOT | Internet of Things |
| IP | Internet Protocol/Intellectual Property |
| ISA | Information Sharing Agency |
| ISO/IEC | International Organization for Standardization/International Electrotechnical Commission |
| IT | Information Technology |
| ITIL | Information Technology Infrastructure Library |
| ITL | Information Technology Laboratory (NIST) |
| JWICS | Joint Worldwide Intelligence Communications System |
| KPI | Key Performance Indicators |
| KRI | Key Risk Indicators |
| KSA | Knowledge, Skills, and Abilities |
| MECE | Mutually Exclusive and Collectively Exhaustive |
| NISPOM | National Industrial Security Program Operating Manual |
| NIST | National Institute of Standards and Technology |
| NCCIC | National Cybersecurity and Communications Integration Center |

| NDI | Non-developmental Items |
|---|---|
| NDIA | National Defense Industrial Association |
| NIAP | National Information Assurance Partnership |
| NICE | National Initiative for Cybersecurity Education |
| NISTIR | National Institute of Standards and Technology Interagency or Internal Report |
| OCONUS | Outside of Continental United States |
| OEM | Original Equipment Manufacturer |
| OGC | Office of the General Counsel |
| OMB | Office of Management and Budget |
| OPSEC | Operations Security |
| OSS | Open Source Solutions |
| OSY | Office of Security |
| OT | Operations Technology |
| OTS | Off-The-Shelf |
| OTTF | Open Group Trusted Technology Forum |
| O-TTPS | Open Trusted Technology Provider™ Standard |
| OWASP | Open Web Application Security Project |
| PACS | Physical Access Control System |
| PII | Personally identifiable information |
| PIV | Personal Identity Verification |
| PM | Program Manager |
| PMO | Program Management Office |
| POA&M | Plan of Action & Milestones |
| QA/QC | Quality Assurance/Quality Control |
| R&D | Research and Development |

| RFI | Request for Information |
|---|---|
| RFP | Request for Proposal |
| RFQ | Request for Questions |
| RMF | Risk Management Framework |
| SAFECode | Software Assurance Forum for Excellence in Code |
| SCIF | Sensitive Compartmented Information Facility |
| SCRM | Supply Chain Risk Management |
| SDLC | System Development Life Cycle |
| SECURE | Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (Technology Act) |
| SLA | Service-Level Agreement |
| SME | Subject Matter Expert |
| SOO | Statement of Objective |
| SOW | Statement of Work |
| SP | Special Publication (NIST) |
| SSP | System Security Plan |
| SWA | Software Assurance |
| SWID | Software Identification Tag |
| TTP | Tactics, Techniques, and Procedures |
| U.S. | United States (of America) |
| US CERT | United States Computer Emergency Readiness Team |

8427

**APPENDIX G: REFERENCES**

[18 U.S.C.]  18 U.S.C. § 2320.

[41 U.S.C.]  41 U.S.C.

[48 C.F.R.]  48 C.F.R.

[ANSI/NASPO]  *ANSI / NASPO Security Assurance Standard*, American National Standards Institute / North American Security Products Organization, 2008.

[ITIL Service Strategy]  Cannon, David, *ITIL Service Strategy*, 2nd Edition, The Stationary Office,, July 29, 2011.

[COSO 2011] Thought Leadership in ERM, *Enterprise Risk Management: Understanding and Communicating Risk Appetite,* Committee of Sponsoring Organization of the Treadway Commission (COSO), 2012, https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf.

[COSO 2020] Thought Leadership in ERM, *Risk Appetite – Critical to Success: Using Risk Appetite To Thrive in a Changing World,* Committee of Sponsoring Organization of the Treadway Commission (COSO), 2020, https://www.coso.org/Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf.

[CISA TEWG] Cybersecurity and Infrasturcture Agency (CISA),  *Information and Communications Technology Supply Chain Risk Management Task Force –  Threat Evaluation Working Group: Threat Scenarios,*Version 2.0, Arlington, Virginia,  2021, https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v2.pdf.

[CISA SCRM WG4] Cybersecurity and Infrastructure Agency (CISA), *Vendor Supply Chain Risk Management (SCRM) Template,* Arlignton, Viriginia, 2021, https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Vendor-SCRM-Template_508.pdf

[Defense Industrial Base Assessment: Counterfeit Electronics]  *Defense Industrial Base Assessment: Counterfeit Electronics,* U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, January 2010, https://www.bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file.

[FEDRAMP]  *FedRAMP*, http://www.fedramp.gov/.

[Gardner]  Gardner, John T. and Cooper, Martha C., "Strategic Supply Chain Mapping Approaches," *Journal of Business Logistics*, 24 (2003),  doi:10.1002/j.2158-1592.2003.tb00045.x.

[GAO] Government Accountability Office (GAO) Report, *Information Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks,* U.S. Government Accountability Office, Washington D.C., 2020, https://www.gao.gov/assets/gao-21-171.pdf.

8476   [IRM[ Institute of Risk Management, *Risk Appetite & Tolerance Guidance Paper*, London, UK, 2011,
8477         https://www.iia.nl/SiteFiles/IRMGuidancePaper-Sep2011.pdf.
8478
8479   [NIAP-CCEVS] *Common Criteria Evaluation & Validation Scheme*, National Information Assurance
8480         Partnership, https://www.niap-ccevs.org/.
8481
8482   [NIST SCRM Proceedings 2012] *Summary of the Workshop on Information and Communication*
8483         *Technologies Supply Chain Risk Management*, Gaithersburg, MD, 2012,
8484         http://www.nist.gov/customcf/get_pdf.cfm?pub_id=913338.
8485
8486   [SwA] *Software Assurance in Acquisition: Mitigating Risks to the Enterprise. A Reference Guide for*
8487         *Security-Enhanced Software Acquisition and Outsourcing,* DoD & DHS SwA Acquisition Working
8488         Group, 2008, https://apps.dtic.mil/dtic/tr/fulltext/u2/a495389.pdf.
8489
8490   [SAFECode 1] Software Assurance Forum for Excellence in Code (Safecode), *Software Integrity*
8491         *Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain*, 2010,
8492         http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf.
8493
8494   [SAFECode 2] Software Assurance Forum for Excellence in Code (Safecode), *The Software Supply*
8495         *Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the*
8496         *Global Supply Chain*, 2009,
8497         http://www.safecode.org/publication/SAFECode_Supply_Chain0709.pdf.
8498
8499   [O-TTPS] The Open Group, Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.1.1,
8500         *Mitigating Maliciously Tainted and Counterfeit Products: Part 1: Requirements and*
8501         *Recommendations*, Open Trusted Technology Provider Standard (O-TTPS), 2018,
8502         https://publications.opengroup.org/c185-1.
8503
8504   [O-TTPS] The Open Group, Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.1.1,
8505         *Mitigating Maliciously Tainted and Counterfeit Products: Part 2: Assessment Procedures for the*
8506         *O-TTPS and ISO/IEC*, Open Trusted Technology Provider Standard (O-TTPS), 2018,
8507         https://publications.opengroup.org/c185-2.
8508
8509   [CNSSI 4009] *National Security Systems (CNSS) Glossary*, April 26, 2010, https://www.serdp-
8510         estcp.org/content/download/47576/453617/file/CNSSI%204009%20Glossary%202015.pdf.
8511
8512   [DHS SSPD 4300A] *Department of Homeland Security (DHS) Sensitive Systems Policy Directive 4300A,*
8513         Department of Homeland Security (DHS), 2011,
8514         http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf.
8515
8516   [DODI 5200.39] Department of Defense Instruction (DODI) 5200.39, *Critical Program Information*
8517         *(CPI) Protection Within the Department of Defense* U.S. Department of Defense, 2010,
8518         https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520039p.pdf.
8519
8520   [FAR]    *Federal Acquisition Regulation (FAR)*, Acquisition Central, https://acquisition.gov/far/.
8521
8522   [FASCA] Federal Acquisition Supply Chain Security Act of 2018 (FASCA), T*itle II of the Strengthening*
8523         *and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE)*
8524         *Technology Act of 2018,* 2018, https://www.congress.gov/115/plaws/publ390/PLAW-
8525         115publ390.pdf.

[FIPS 199]  Federal Information Systems Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[FIPS 200]  Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, 2006, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[FSP] The Profile Version 1.0, *Financial Services Cybersecurity Framework Profile Version 1.0,* Cyber Risk Institute, 2020, https://cyberriskinstitute.org/the-profile/.

[ISO 9000]  ISO 9000:2015, *Quality Management — Fundamentals and vocabulary*, International Organization for Standardization, 2018, https://www.iso.org/standard/45481.html.

[ISO 9001]  ISO 9001:2018, *Quality management systems — Requirements,* International Organization for Standardization, 2018,  https://www.iso.org/standard/62085.html.

[ISO 28000]  ISO 28000:2007, *Specification for Security Management Systems for the Supply Chain*, International Organization for Standardization, 2007, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44641.

[ISO 28001]  ISO 28001:2007, *Security management systems for the supply chain -- Best practices for implementing supply chain security, assessments and plans -- Requirements and guidance*, International Organization for Standardization, 2007, http://www.iso.org/iso/catalogue_detail?csnumber=45654.

[ISO/IEC 2382]  ISO/IEC 2382-36:2013, *Information Technology -- Vocabulary*, International Organization for Standardization / International Electrotechnical Commission, 2013, http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63598.

[ISO/IEC 12207]  ISO/IEC 12207: 2017, *Systems and software engineering -- Software life cycle processes*, International Organization for Standardization / International Electrotechnical Commission, 2017, https://www.iso.org/standard/63712.html.

[ISO/IEC 15288]  ISO/IEC 15288:2015, *Systems and software engineering -- System life cycle processes*, International Organization for Standardization / International Electrotechnical Commission, 2015, https://www.iso.org/standard/63711.html.

[ISO/IEC 27000]  ISO/IEC 27000:2014, *Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary*, International Organization for Standardization / International Electrotechnical Commission, 2014, http://www.iso.org/iso/catalogue_detail?csnumber=41933.

[ISO/IEC 27001]  ISO/IEC 27001:2013, *Information technology -- Security techniques -- Information security management systems -- Requirements*, International Organization for Standardization / International Electrotechnical Commission, 2013, http://www.iso.org/iso/catalogue_detail?csnumber=54534.

[ISO/IEC 27002]  ISO/IEC 27002:2013, *Information technology -- Security techniques -- Code of practice for information security controls*, International Organization for Standardization / International Electrotechnical Commission, 2013, http://www.iso.org/iso/catalogue_detail?csnumber=54533.

[ISO/IEC 27036]  ISO/IEC 27036-2:2014, *Information technology -- Security techniques -- Information security for supplier relationships*, International Organization for Standardization / International Electrotechnical Commission, 2014, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=59680.

[ISO/IEC 20243] ISO/IEC 20243:2018, – *Information Technology — Open Trusted Technology Provider^TM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products,* International Organization for Standardization / International Electrotechnical Commission, 2018, https://www.iso.org/standard/74399.html.

[IRM] Institute of Risk Management, *Risk Appetite & Tolerance Guidance Paper,* London, 2011 https://www.iia.nl/SiteFiles/IRMGuidancePaper-Sep2011.pdf

[NDIA]  National Defense Industrial Association (NDIA) System Assurance Committee, *Engineering for System Assurance*, NDIA, Arlington, VA, 2008, https://www.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/systems-engineering/sse-committee/systems-assurance-guidebook.ashx.

[NISPOM]  DoD 5220.22-M: *National Industrial Security Program - Operating Manual (NISPOM),* Department of Defense, 2006, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodm/522022m.pdf.

[NIST CSF]  *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1, National Institute of Standards and Technology, Gaithersburg, MD, 2018,

[NISTIR 7622]  NIST Interagency Report (IR) 7622: *Notional Supply Chain Risk Management Practices for Federal Information Systems,* National Institute of Standards and Technology, Gaithersburg, MD, 2012, http://dx.doi.org/10.6028/NIST.IR.7622.

[NISTIR 8179]  NIST Interagency Report (IR) 8179: *Criticality Analysis Process Model Prioritizing Systems and Component,* National Institute of Standards and Technology, Gaithersburg, MD, 2018, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf.

[NISTIR 8272]  NIST Interagency Report (IR) 8272: *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks,* National Institute of Standards and Technology, Gaithersburg, MD, 2020, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8272.pdf.

[NISTIR 8276]  NIST Interagency Report (IR) 8276: *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry,* National Institute of Standards and Technology, Gaithersburg, MD, 2021, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf.

[NISTIR 8286]  NIST Interagency Report (IR) 8286: *Integrating Cybersecurity and Enterprise Risk Management (ERM),* National Institute of Standards and Technology, Gaithersburg, MD, 2020, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf.

[NIST SP 800-30 Rev. 1]  NIST Special Publication (SP) 800-30 Revision 1, *Guide for Conducting Risk Assessments,* National Institute of Standards and Technology, Gaithersburg, MD, 2012, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[NIST SP 800-32]  NIST Special Publication (SP) 800-32: *Introduction to Public Key Technology and the Federal PKI Infrastructure,* National Institute of Standards and Technology, Gaithersburg, MD, 2001, http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf.

[NIST SP 800-34 Rev. 1]  NIST Special Publication (SP) 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems,* National Institute of Standards and Technology, Gaithersburg, MD, 2010, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf.

[NIST SP 800-37]  NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* National Institute of Standards and Technology, Gaithersburg, MD, 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[NIST SP 800-39]  NIST Special Publication (SP) 800-39, *Managing Information Security Risk,* National Institute of Standards and Technology, Gaithersburg, MD, 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[NIST SP 800-53 Rev. 5]  NIST Special Publication (SP) 800-53 Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* National Institute of Standards and Technology, Gaithersburg, Maryland, 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[NIST SP 800-53A Rev. 4]  NIST Special Publication (SP) 800-53A Revision 4, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans,* National Institute of Standards and Technology, Gaithersburg, MD, 2014, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

[NIST SP 800-53B Rev. 5] NIST Special Publication (SP) 800-53B Revision 5, *Control Baselines for Information Systems and Organizations*, National Institute of Standards and Technology, Gaithersburg, Maryland, 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

[NIST SP 800-100]  NIST Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Managers,* National Institute of Standards and Technology, 2006, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

[NIST SP 800-115]  NIST Special Publication (SP) 800-115, *Technical Guide to Information Security Testing and Assessment,* National Institute of Standards and Technology, Gaithersburg, MD, 2008, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

[NIST SP 800-160 Vol. 1]  NIST Special Publication (SP) 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* National Institute of Standards and Technology, Gaithersburg, MD, 2016, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf.

8674
8675    [NIST SP 800-181 Rev. 1] NIST Special Publication (SP) 800-181, *Workforce Framework for*
8676        *Cybersecurity (NICE Framework),* National Institute of Standards and Technology, Gaithersburg,
8677        MD, 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.
8678
8679    [OMB A-76]  OMB Circular A-76, *Performance of Commercial Activities,* Office of Management and
8680        Budget, 2003,
8681        https://obamawhitehouse.archives.gov/omb/circulars_a076_a76_incl_tech_correction/.
8682
8683
8684
8685