CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) PLAN

NIST SP 800-161 Rev 1
C-SCRM Plan Format

System Name: [system name]
Contractor's Name: [name & address]
C-SCRM Plan Date of Issue: [date]
Contract Number: [contract #]

SENSITIVE
Access Limited to Authorized Personnel

NOTICE

ACME Business Consulting, LLP (ACME) uses this Cybersecurity Supply Chain Risk Management (C-SCRM) Plan to define holistic approach to C-SCRM activities, involving all supply chain stakeholders, which identifies, assesses, handles and monitors supply chain risks associated with weaknesses, vulnerabilities and threats, addressing both services and products.

ACME's approach to C-SCRM is an enterprise-wide activity that is implemented throughout the System Development Life Cycle (SDLC). Proactive SDLC practices help ACME minimize supply chain-related risks associated with systems, system components and/or system services that include:[1]

1. Research and development;[2]
2. Design;[3]
3. Manufacturing;[4]
4. Acquisition;[5]
5. Delivery;[6]
6. Integration;[7]
7. Operations; [8]
8. Maintenance;[9] and
9. Disposal.[10]

The format of this C-SCRM Plan contains information to adhere to NIST SP 800-161 Rev 1 (Appendix D.3).[11]

[1] *NIST SP 800-161 R1: https://csrc.nist.gov/pubs/sp/800/161/r1/final| NIST SP 800-171A R3: A.03.17.01.a[01]*
[2] *NIST SP 800-171A R3: A.03.17.01.a[02]*
[3] *NIST SP 800-171A R3: A.03.17.01.a[03]*
[4] *NIST SP 800-171A R3: A.03.17.01.a[04]*
[5] *NIST SP 800-171A R3: A.03.17.01.a[05]*
[6] *NIST SP 800-171A R3: A.03.17.01.a[06]*
[7] *NIST SP 800-171A R3: A.03.17.01.a[07]*
[8] *NIST SP 800-171A R3: A.03.17.01.a[08]*
[9] *NIST SP 800-171A R3: A.03.17.01.a[09]*
[10] *NIST SP 800-171A R3: A.03.17.01.a[10]*
[11] *NIST SP 800-161 Rev 1 - https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final*

Table of Contents

ACME uses this Cybersecurity Supply Chain Risk Management (C-SCRM) Plan to define holistic approach to C-SCRM activities, involving all supply chain stakeholders, which identifies, assesses, handles and monitors supply chain risks associated with weaknesses, vulnerabilities and threats, addressing both services and products. The format of this C-SCRM Plan contains information to adhere to NIST SP 800-161 Rev 1 (Appendix D.3).[12]

SYSTEM NAME & IDENTIFIER

This C-SCRM plan provides an overview of the security requirements for the [system name] [unique identifier] and describes the supply chain cybersecurity controls in place or planned for implementation to provide fit-for-purpose C-SCRM controls that are appropriate for the information to be transmitted, processed or stored by the system. The security safeguards implemented for the [unique identifier] meet the requirements set forth in ACME's C-SCRM strategy and policy guidance.

SYSTEM DESCRIPTION

[describe the function, purpose and scope of the system and include a description of the information processed. Provide a general description of the system's approach to managing 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 that the C-SCRM plan describes the system in the context of ACME'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 and business functions of the system; the authorization boundary of the system; the overall system architecture, including any supporting systems and relationships; how the system supports enterprise missions; and the system environment (e.g., stand-alone, managed/enterprise, custom/specialized, security-limited functionality, cloud).]

SYSTEM INFORMATION TYPE AND CATEGORIZATION

The following tables specify the information types that are processed, stored or transmitted by [system name] and/or its in-boundary supply chain. Using guidance regarding the categorization of assets, ACME determines the security impact levels for each information type:

- Per NIST FIPS Pub 199, Controlled Unclassified Information (CUI) is MODERATE confidentiality;
- Per NIST FIPS Pub 200, CUI is MODERATE impact; and
- Availability for CUI determinations it out-of-scope for FIPS 199, FIPS 200 and NIST SP 800-171.

Information Type	Security Objectives		
	Confidentiality (low, mod or high)	**Integrity** (low, mod or high)	**Availability** (low, mod or high)
Federal Contract Information (FCI)	Low	Low	N/A
Controlled Unclassified Information (CUI)	Moderate	Moderate	N/A

Based on the table above, the "high-water mark" for each of the security impacts (e.g., low, moderate, high) determines the overall system categorization. [system name] has MODERATE security objectives.

Security Objective	Security Impact Level		
	Low	**Moderate**	**High**
Confidentiality	☐	☒	☐
Integrity	☐	☒	☐
Availability	☐	☒	☐

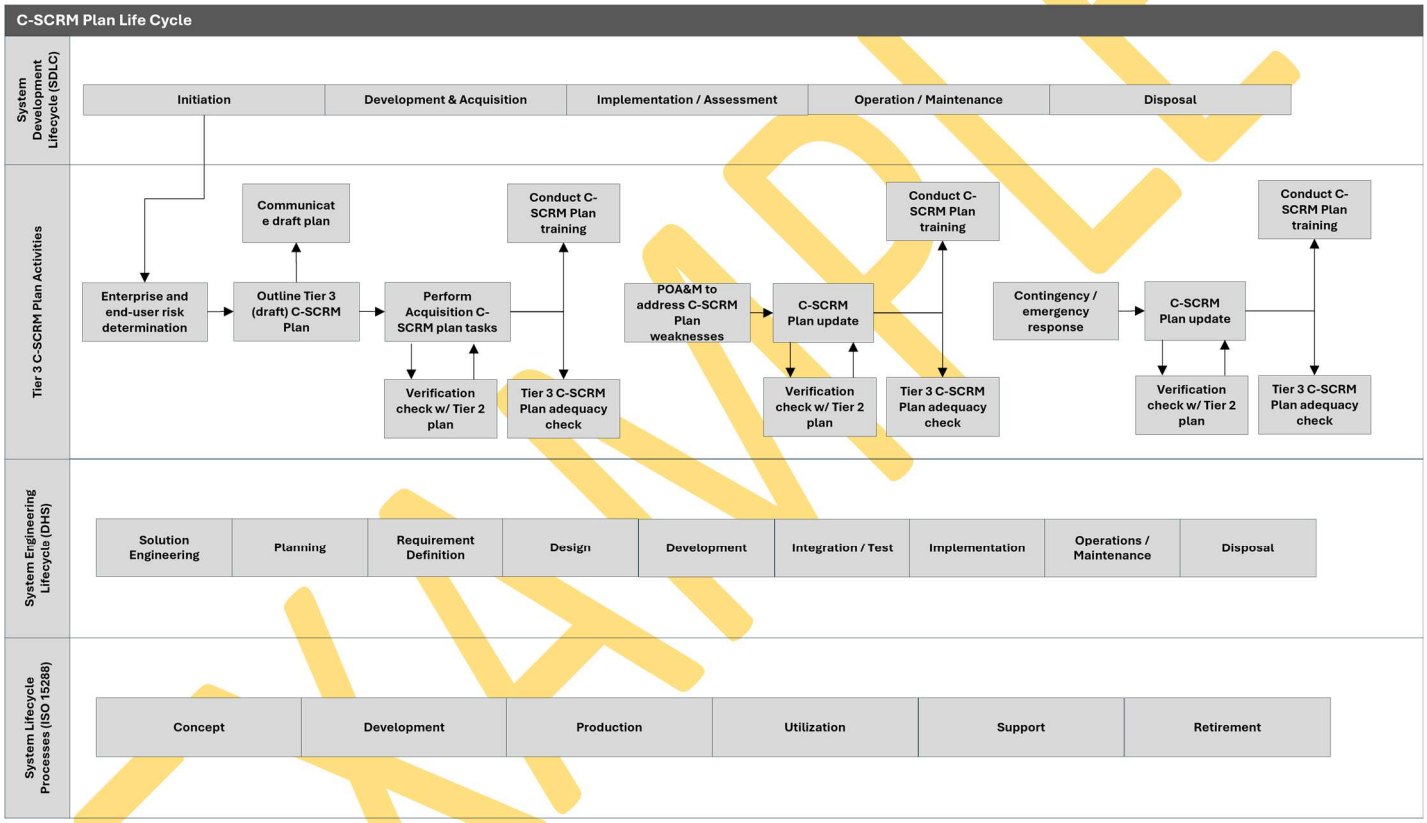
[12] *NIST SP 800-161 Rev 1 - https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final*

C-SCRM Plan & Life Cycles

[describe how C-SCRM plan activities should be integrated into ACME's system and software life cycle processes.]

[system name]'s C-SCRM Plan cover the full life cycle of in-scope components (e.g., people, processes, technology, data and facilities), including:

- Research and Development (R&D);
- Design;
- Manufacturing;
- Acquisition;
- Delivery;
- Integration;
- Operations; and
- Disposal/retirement.



Cybersecurity Supply Chain Risk Assessment (C-SCRA)

The expression "cybersecurity supply chain risk assessment" should be considered equivalent to "supply chain risk assessment" in an effort to harmonize terminology. The Cybersecurity Supply Chain Risk Assessment (C-SCRA) is meant to guide the review of any third-party product, service or supplier (e.g., Suppliers, Integrators and Service Providers (SISP)) that could present a cybersecurity risk to ACME.

ACME's C-SCRA template provides a toolbox of questions that ACME can choose to use or not use depending on the controls selected. The C-SCRA considers available public and private information to perform a holistic assessment, including known cybersecurity risks throughout the supply chain, the likelihoods of their occurrence and their potential impacts on an enterprise and its information and systems.

ACME's C-SCRA is intended to fairly and consistently evaluate risks posed to via third parties that hold the potential for harm or compromise as a result of cybersecurity risks. Requestors seeking to introduce SISP into ACME's C-SCRA process contains five (5) primary steps:

1. Information Gathering and Scoping Analysis;

APPENDIX A – C-SCRM CONTROL DETAILS

ACME selected the C-SCRM Baseline set of controls from NIST SP 800-161 Rev 1, since the C-SCRM Baseline is designed to addresses the basic needs of a broad and diverse set of businesses. As necessary, ACME will select, tailor and implement additional security controls based on:

- The environments in which ACME information systems are acquired and operate;
- The nature of ACME's operations;
- The types of threats facing ACME's:
  - Business operations;
  - Mission;
  - Supply chains; and
  - Information systems; and
- The type of information processed, stored or transmitted by information systems and the supply chain infrastructure.

AC-1 - POLICY AND PROCEDURES

Summary C-SCRM Control Implementation
Implementation Status (check all that apply): ☐ Implemented (control execution internal to ACME) ☐ Implemented (control execution external to ACME via contract and/or shared responsibility) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable
Process Owner: [name of the individual or team accountable for the procedure being performed]
Process Operator: [name of the individual or team responsible to perform the procedure's tasks]
Occurrence: [how often the procedure need is performed]
Location of Additional Documentation: [location where additional documentation can be found, e.g., policies, standards, procedures and other evidence]
Technology in Use: [if applicable, the name of the application/system/service used to perform the procedure]
Description of Control Implementation: Supporting policy: [insert policy name] Supporting standard: [insert standard name] Supporting procedure: [insert procedure name] [briefly describe the how this control is implemented]

AC-2 - ACCOUNT MANAGEMENT

Summary C-SCRM Control Implementation
Implementation Status (check all that apply): ☐ Implemented (control execution internal to ACME) ☐ Implemented (control execution external to ACME via contract and/or shared responsibility) ☐ Partially Implemented *(Identified in POA&M)* ☐ Planned *(Identified in POA&M)* ☐ Alternative Implementation *(Compensating Controls)* ☐ Not applicable