SUPPLY CHAIN RISK MANAGEMENT (SCRM) PLAN

DI-MGMT-82256A
SCRM Plan Format

SCRM Plan Date of Issue: [date]
SCRM Plan Document Number: [document #]
Contract Number: [contract #]
Contractor's Name and Address: [name & address]
Title of Plan: [project or company-specific SCRM Plan title]
Program Title: [program title]
Security Classification: [US government security classification]
USD(R&E) Critical Technology List (if applicable): [CTL description]
Distribution Statement: [distribution statement]
Destruction Notice (if applicable): [destruction notice]
Cybersecurity Maturity Model Certification (CMMC) Certification Level: [CMMC level]

Table of Contents

Notice 3
SCRM Plan Revision Control 4
Scope 5
SCRM Applicability 5
Statutory Requirements 5
Regulatory Requirements 5
Contractual Requirements 6
Holistic SCRM Approach 6
Description of Linked Supply Chain Activities 7
SCRM Strategy 8
Responsible Organizational Component 9
SCRM-Specific Organization Chart 9
SCRM Primary and Alternate Points of Contact (POC) 9
Primary POC 9
Alternate POC 10
SCRM Processes and Procedures 11
SCRM Process Description 11
Include SCRM in Market Research 12
Include SCRM in Source Selection Technical Evaluations 12
Validate/Audit Deliverables 13
Document/Update SCRM in Acquisition Documents 13
Conduct Supply Chain Threat Assessments 13
Obtain Supplier and Performance Information 13
Threat Assessment 13
Conduct Hardware, Software & Firmware Assurance 13
Conduct Hardware, Software, Firmware & Cybersecurity Vulnerability Analysis 13
Perform a Discrete Supplier Review (DSR) To Address Supplier Concerns 14
Leverage Commercial Supply Chain Tools 15
Create A Risk Handling Plan 15
Conduct Continuous Supply Chain Risk Monitoring 15
SCRM Plan Update Process 15
Supply Chain Risk Identification 16
Processes & Tools 16
Intelligence-Based Techniques To Uncover & Map Supplier Networks 16
Process For Communicating Supply Chain Risks To Affected Stakeholders 16
Supply Chain Risk Assessment 17
Process To Scan Supply Chain Network 17
Methodology for Assessing Vendors or Sources of Supply 17
Root Cause Analysis (RCA) Process 17
Supply Chain Risk Register Governance 17
Supply Chain Risk Register Reporting 18
Supply Chain Risk Handling 19
Supply Chain Risk Handling Plans 19
Methodology To Prioritize Potential Supply Chain Risks 19
Supply Chain Risk Register Entries 20
Supply Chain Risk Monitoring 21
Supply Chain Risk Monitoring & Handling Plans 21
Supply Chain Risk Reporting 21
Supply Chain Risk Register Process 22
SCRM Training 23
SCRM Training Overview 23
SCRM Course Catalog 23
SCRM Training Metrics 23
Role-Based SCRM Training 23

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 SCRM Plan adheres to the US Government's Data Item Description (DID) DI-MGMT-82256A for the format, content and intended use information.[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] *DI-MGMT-82256 Revision A - https://quicksearch.dla.mil/qsDocDetails.aspx?ident_number=283181*

SCOPE

Per DI-MGMT-82256A, this section shall include:

(1) Defining SCRM applicability to the prime and all suppliers, subcontractors, associated integrators, and vendors;

(2) Defining SCRM as the coordinated, holistic approach, 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; and

(3) Defining the supply chain as the linked activities associated with providing materiel from a raw material stage to an end user as a finished product.

SCRM APPLICABILITY

[edit the section below to define the applicability of this SCRM Plan as it pertains to the prime and all suppliers, subcontractors, associated integrators, and vendors.]

This document addresses ACME Business Consulting, LLP's (ACME) Supply Chain Risk Management Plan (SCRM Plan).

ACME has compliance obligations that where applicable, must "flow down" to the ensure Suppliers, Integrators and Service Providers (SISP) via contractual obligations, based on the roles & responsibilities of the SISP, specific to the business case and technology-related implications.

STATUTORY REQUIREMENTS

[edit the section below to fill-in applicable statutory requirements]

ACME's statutory requirements include:

- Children's Online Privacy Protection Act (COPPA)
- Computer Fraud and Abuse Act (CFAA)
- Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)
- Electronic Communications Privacy Act (ECPA)
- Fair & Accurate Credit Transactions Act (FACTA)
- Fair Credit Reporting Act (FCRA)
- Family Education Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FISMA)
- Federal Trade Commission Act (FTCA)
- Gramm Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes Oxley Act (SOX)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
- US State - Massachusetts 201 CMR 17.00
- US State - Oregon Identity Theft Protection Act (ORS 646A)
- International - United Kingdom Data Protection Act (UK DPA)

REGULATORY REQUIREMENTS

[edit the section below to fill-in applicable regulatory requirements]

ACME's regulatory requirements include:

- Cybersecurity Maturity Model Certification (CMMC)
- Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7008, 252.204-7012, 252.204-7019, 252.204-7020, 252.204-7021, etc.
- Department of Defense Information Assurance Risk Management Framework (DIARMF) (DoDI 8510.01)
- Federal Acquisition Regulation (FAR 52.204-21)
- Federal Risk and Authorization Management Program (FedRAMP)
- European Union General Data Protection Regulation (EU GDPR)
- Financial Industry Regulatory Authority (FINRA)
- National Industrial Security Program Operating Manual (NISPOM)

- New York Department of Financial Services (NY DFS) 23 NYCCRR 500
- North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

CONTRACTUAL REQUIREMENTS

[edit the section below to fill-in applicable contractual requirements]

ACME's contractual requirements include:

- American Institute of CPAs Service Organization Control (AICPA SOC2)
- Center for Internet Security Critical Security Controls (CIS CSC)
- Cloud Security Alliance Cloud Controls Matrix (CSA CCM)
- Payment Card Industry Data Security Standard (PCI DSS)

HOLISTIC SCRM APPROACH

[edit the section below to define how ACME's approach to SCRM is coordinated and holistic, 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 SCRM is an enterprise-wide activity that is implemented throughout the System Development Life Cycle (**SDLC**). Proactive SDLC practices will help ACME minimize supply chain-related risks associated with systems, system components and/or system services that include:[12]

10. Research and development;[13]
11. Design;[14]
12. Manufacturing;[15]
13. Acquisition;[16]
14. Delivery;[17]
15. Integration;[18]
16. Operations; [19]
17. Maintenance;[20] and
18. Disposal.[21]

From a practical standpoint, implementing a SCRM capability it is more than just a control set. The successful implementation of ACME's SCRM Plan requires a certain level of delegated authority over key business functions that impact supply chain security:

- Secure Development Practices;
- Procurement Practices;
- Risk Management Practices; and
- Systems, Applications & Services Management Practices.

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, is the "gold standard" for C-SCRM-related concepts and ACME's C-SCRM SIP considerably relies on that body of work.[22]

---

[12] *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]*
[13] *NIST SP 800-171A R3: A.03.17.01.a[02]*
[14] *NIST SP 800-171A R3: A.03.17.01.a[03]*
[15] *NIST SP 800-171A R3: A.03.17.01.a[04]*
[16] *NIST SP 800-171A R3: A.03.17.01.a[05]*
[17] *NIST SP 800-171A R3: A.03.17.01.a[06]*
[18] *NIST SP 800-171A R3: A.03.17.01.a[07]*
[19] *NIST SP 800-171A R3: A.03.17.01.a[08]*
[20] *NIST SP 800-171A R3: A.03.17.01.a[09]*
[21] *NIST SP 800-171A R3: A.03.17.01.a[10]*
[22] *NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf*

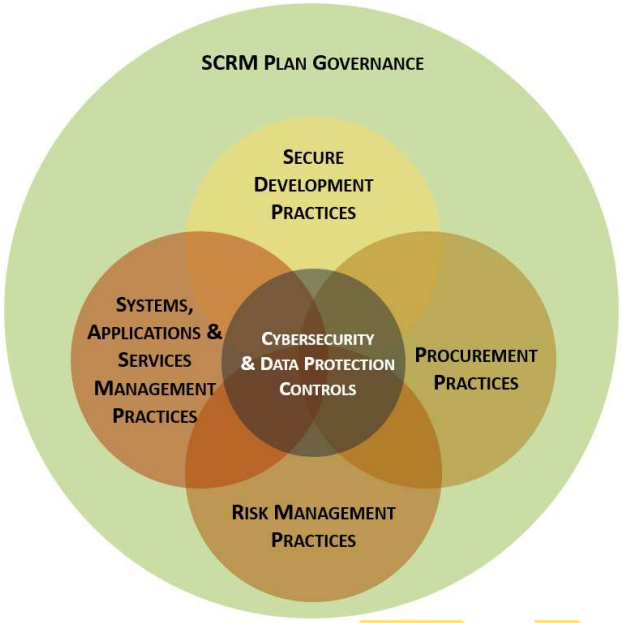

Figure 1. SCRM Organizational Components

Within the concept of secure development practices, in order to ensure C-SCRM is operational it takes the following to exist and be functional:

- Maintain close working relationships through frequent visits and communications.
- Mentor and coach suppliers on C-SCRM and actively help suppliers improve their cybersecurity and supply chain practices.
- Invest in common solutions.
- Require the use of the same standards within the acquirer organizations and by suppliers, thereby simplifying communications about cybersecurity risk and mitigations and helping to achieve a uniform level of quality throughout the ecosystem.
- Restrict the use of open-source software to projects for which there is clear oversight and accountability. If this is not possible, then code audits/reviews should be performed for open-source project.

Resilience and improvement activities include:

- Rules and protocols for information sharing between acquirers and suppliers.
- Joint development, review and revision of incident response, business continuity and disaster recovery plans.
- Protocols for communicating vulnerabilities and incidents.
- Responsibilities for responding to cybersecurity incidents.
- Coordinated communication methods and protocols.
- Coordinated restoration and recovery procedures.
- Collaborative processes to review lessons learned.
- Updates of coordinated response and recovery plans based on lessons learned.

Description of Linked Supply Chain Activities

[edit the section below to define the linked activities of the supply chain that are associated with providing materiel from a raw material stage to an end user as a finished product.]

To be defined by ACME subject matter experts who can answer the specifics of supply chain activities specific to ACME's business operations.