Your Logo
Will Be
Placed Here

SUPPLY CHAIN RISK MANAGEMENT (SCRM)

THIRD-PARTY SERVICE PROVIDER (TSP) SECURITY REQUIREMENTS

ACME Business Consulting, LLC

SCRM
Supply Chain Risk Management

REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

ACME's Supply Chain Risk Management (SCRM) program references numerous leading industry frameworks in an effort to provide a comprehensive and holistic approach to identifying, managing and remediating supply-chain related threats and risks. With the intent to incorporate both security and privacy concepts in all stages of the supply chain and System Development Life Cycle (SDLC), the following external content is referenced by or supports this document:

- National Institute of Standards and Technology (**NIST**): [1]
  - NIST SP 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems*
  - NIST SP 800-39: *Managing Cybersecurity Risk: Organization, Mission and Information System View*
  - NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
  - NIST SP 800-63-3: *Digital Identity Guidelines*
  - NIST SP 800-64: *Security Considerations in System Development Lifecycle*
  - NIST SP 800-122: *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
  - NIST SP 800-128: *Guide for Security-Focused Configuration Management of Information Systems*
  - NIST SP 800-160 vol1: *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*
  - NIST SP 800-160 vol2: *Developing Cyber Resilient Systems: A Systems Security Engineering Approach*
  - NIST SP 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
  - NIST SP 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
  - NIST SP 800-172: *Enhanced Security Requirements for Protecting CUI: A Supplement to NIST SP 800-171*
  - NIST SP 800-207: *Zero Trust Architecture (ZTA)*
  - NIST IR 8062: *An Introduction to Privacy Engineering and Risk Management in Federal Systems*
  - NIST IR 8179: *Criticality Analysis Process Model: Prioritizing Systems and Components* [draft]
  - NIST *Framework for Improving Critical Cybersecurity* (Cybersecurity Framework)
- International Organization for Standardization (**ISO**):[2]
  - ISO 15288: *Systems and Software Engineering - System Life Cycle Processes*
  - ISO 27001: *Information Technology - Security Techniques - Information Security Management Systems - Requirements*
  - ISO 27002: *Information Technology - Security Techniques - Code of Practice for Cybersecurity Controls*
  - ISO 27018: *Information Technology - Security Techniques - Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors*
- Other Frameworks:
  - Cybersecurity Maturity Model Certification (**CMMC**)[3]
  - Secure Controls Framework (**SCF**) [4]
  - SCF Security & Privacy Risk Management Model (**SP-RMM**)
  - SCF Security & Privacy Capability Maturity Model (**SP-CMM**)
  - Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)[5]
  - Center for Internet Security (**CIS**)[6]
  - Open Web Application Security Project (**OWASP**)[7]
  - Department of Defense Cybersecurity organizational (**DISA**) Secure Technology Implementation Guides (**STIGs**)[8]
  - Fair Information Practice Principles (**FIPP**)[9]
  - European Union Regulation 2016/279 (General Data Protection Regulation (**EU GDPR**))[10]
  - Payment Card Industry Data Security Standard (**PCI DSS**)[11]

[1] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[2] International Organization for Standardization - https://www.iso.org
[3] Office of the Under Secretary of Defense for Acquisition & Sustainment - https://www.acq.osd.mil/cmmc/draft.html
[4] Secure Controls Framework - https://www.securecontrolsframework.com
[5] Cloud Security Alliance - https://cloudsecurityalliance.org/
[6] Center for Internet Security - https://www.cisecurity.org/
[7] Open Web Application Security Project - https://www.owasp.org/index.php/Main_Page
[8] DoD Information Security organizational - http://iase.disa.mil/stigs/Pages/index.aspx
[9] Federal Trade Commission - https://www.ftc.gov
[10] EU General Data Protection Regulation - http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
[11] Payment Card Industry Security Standards Council - https://www.pcisecuritystandards.org/

Table of Contents

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT PROGRAM REQUIREMENTS

ACME Business Consulting, LLC (ACME) must implement appropriate measures to ensure Third-Party Service Providers (TSP) (term that includes suppliers, contractors, consultants, interns and other entities that make up the supply chain) protect the confidentiality, integrity, availability and safety of ACME technology assets. These measures apply regardless of how data is created, processed, transmitted and/or stored across systems, services and applications. ACME must tailor cybersecurity and data protection controls accordingly so that cost-effective controls can be applied, commensurate with the risk and sensitivity of the data, in accordance with all statutory, regulatory and contractual obligations.

ACME's Management Intent For Supply Chain Risk Management (SCRM): The successful implementation of ACME's cybersecurity and data protection program depends on the successful implementation and proactive governance of not just ACME's security and privacy controls, but also those that are either entirely, or a shared, responsibility of each TSP that makes up ACME's supply chain. Within the scope of ACME's supply chain, the cybersecurity and data protection program of each TSP directly impacts ACME. Therefore, clear requirements in the form of legally-binding contracts are necessary to avoid inaccurate assumptions on roles and responsibilities for the shared security of ACME's technology assets. ACME's SCRM program can provide a list of requirements to add as contract addendums for the "flow down" of specific cybersecurity and data protection requirements to TSPs.

MANAGEMENT DIRECTION FOR THIRD-PARTY CYBERSECURITY PRACTICES

The objective of the Supply Chain Risk Management (SCRM) program is to provide direction for managing cybersecurity and privacy requirements as it pertains to ACME's supply chain that is based on NIST SP 800-161 practices.[12] The SCRM program is authorized and supported by ACME's executive leadership.

ACME is committed to protecting its employees, partners, clients and ACME from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every entity that interacts with ACME data and systems, applications and services. Therefore, it is the responsibility of both ACME personnel and TSPs to be aware of and adhere to ACME's cybersecurity and data protection requirements.

Protecting ACME data and the systems that collect, process and maintain this data is of critical importance. Commensurate with risk, security and privacy measures must be implemented to guard against unauthorized access to, alteration, disclosure or destruction of data and systems, applications and services. This also includes protection against accidental loss or destruction. The security of systems, applications and services must include controls and safeguards to offset possible threats, as well as controls to ensure confidentiality, integrity, availability and safety:

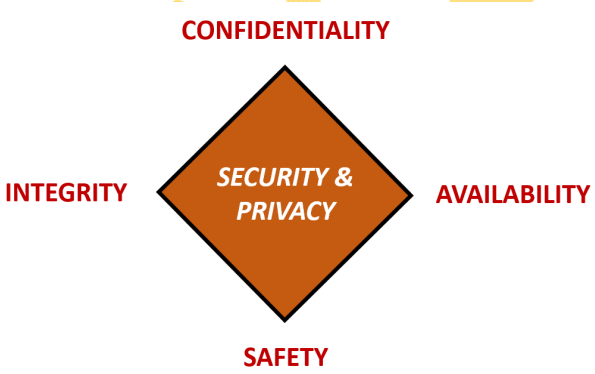

Figure 1: CIAS Model

- **CONFIDENTIALITY** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **INTEGRITY** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- **AVAILABILITY** – Availability addresses ensuring timely and reliable access to and use of information.
- **SAFETY** – Safety addresses reducing risk associated with embedded technologies that could fail or be manipulated by nefarious actors.

[12] NIST SP 800-161 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

SUPPLY CHAIN RISK MANAGEMENT (SCRM) CONSIDERATIONS

Supply Chain Risk Management (SCRM) is meant to identify, assess and mitigate risks associated with the global and distributed nature of ACME's technology-related product and service supply chains.[15] This document empowers ACME's management team to develop supply chain-related mitigation strategies that are tailored to the particular mission/business needs, threats and operational environments.

DEFINING THE SUPPLY CHAIN

ACME's technology-related supply chain infrastructure is the integrated set of components (e.g., hardware, software and processes) that composes the environment in which a system, application or service is developed, manufactured, tested, deployed, maintained and/or and retired/decommissioned. Therefore, ACME's SCRM must incorporate security and privacy concepts in all stages of the System Development Life Cycle (SDLC).

IDENTIFYING THE PROBLEM WITH SUPPLY CHAIN-RELATED TECHNOLOGY RISKS

ACME's supply chain risks are associated with decreased visibility into and understanding of, how the technology and services that ACME acquires is developed, integrated and deployed.

ACME's Business Process Owners (BPOs) must address the realities of the supply chain when evaluating risks, since just as ACME relies on Third-Party Service Providers (TSP), so do those businesses that make up our supply chain. Traditionally, the immediate TSP receives the highest levels of scrutiny, with diminishing levels of both visibility and scrutiny along each additional "hop" within the supply chain. This lack of visibility into the risks associated with the supply chain pose a significant challenge to ACME's SCRM activities.

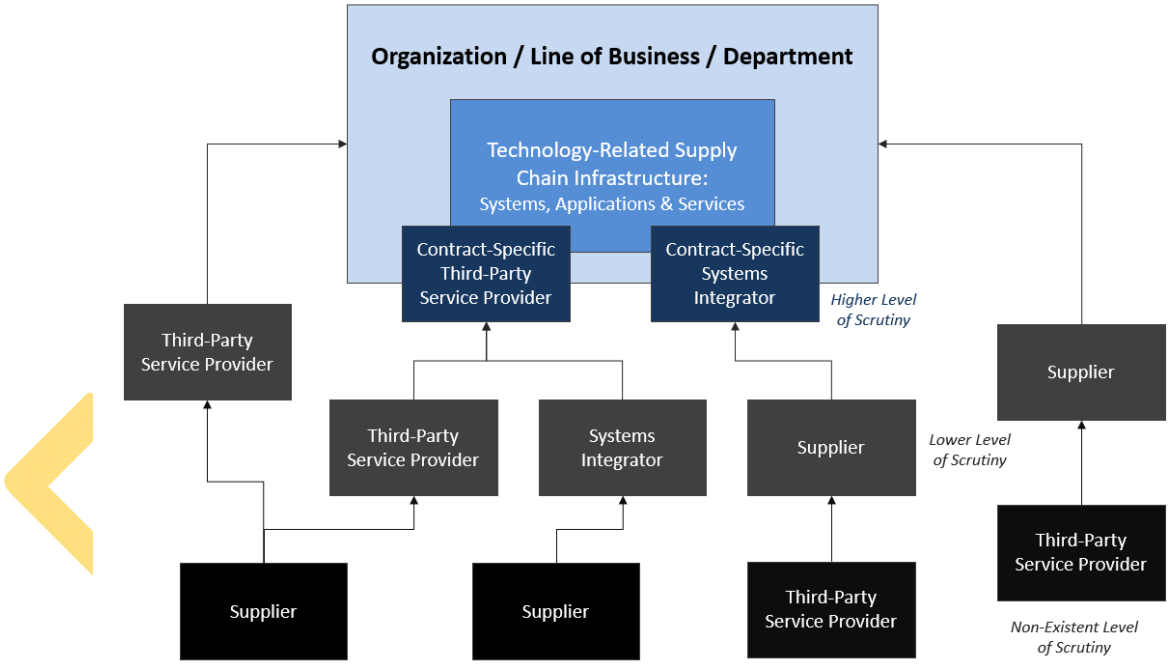

Figure 3: Nested Supply Chain Dependencies

[15] NIST SP 800-161 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Examples of evaluating supply chain deficiencies against the risk tiers:

Risk Tier	Deficiency Example	Possible Mitigation
1 Strategic	1. Deficiencies or weaknesses in TSP governance structures or processes such as a lack of a formal cybersecurity and data protection program.	1. Seek out alternate sources, including insourcing the requirement, since building a cybersecurity and data protection program takes considerable time.
2 Operational	1. TSP has no operational process is in place for detecting counterfeits in its supply chain. 2. TSP is susceptible to using unofficial supply sources. 3. TSP lacks required certifications.	1. TSP must develop a program for detecting counterfeits and allocate appropriate budgets for putting in resources and training. 2. TSP must demonstrate it only purchases through official supply sources to minimize the risk of counterfeit products. 3. TSP must earn required certifications (e.g., CMMC Level 3) in the necessary timeline or seek out alternative sources.
3 Tactical	1. Discrepancy in system functions does not meet ACME requirements, resulting in substantial impact to performance or gap in security functionality.	1. TSP must initiate an engineering change to address both technical and business requirements.

SCRM Risk Management Steps

In accordance with industry-recognized secure practices, ACME's SCRM program incorporates the traditional "Plan-Do-Check-Act" (PDCA), or Deming Cycle, approach to identify, evaluate and mitigate risks. This involves:

- Plan: Designing the SCRM, assessing IT-related risks and selecting appropriate controls.
- Do: Implementing and operating the appropriate security controls.
- Check: Reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- Act: Making changes, where necessary, to bring the SCRM back to optimal performance.

SCRM is integrated into ACME's organization-wide Risk Management Program (RMP). The process associated with managing SCRM-related risks include the following continuous and iterative steps:

1. Frame Risk. Establish the context for risk-based decisions and the current state of the technology assets or supply chain infrastructure;
2. Assess Risk. Review and interpret criticality, threat, vulnerability, likelihood, impact and related information;
3. Respond to Risk. Select, tailor and implement mitigation controls; and
4. Monitor Risk. On an ongoing basis, risk needs to be monitored, including changes to technology assets or supply chain infrastructure, using effective organizational communications and a feedback loop for continuous improvement.

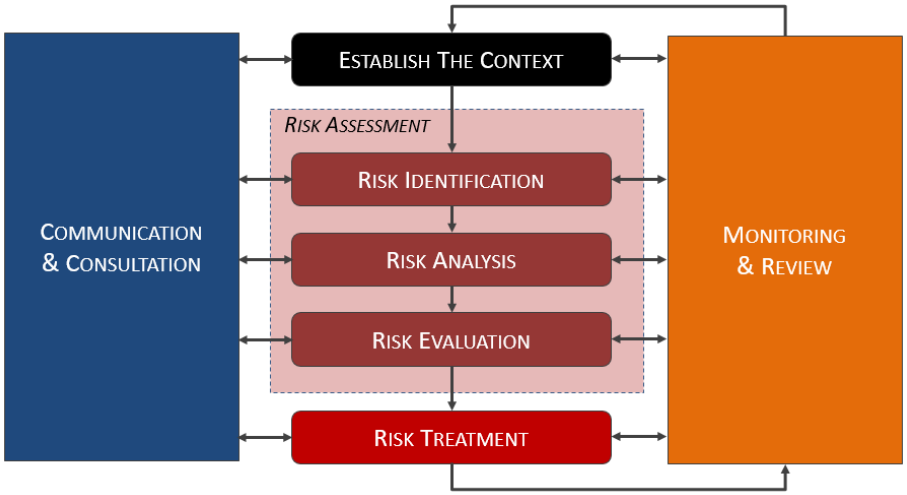

Figure 5: NIST SP 800-161 & ISO 31010 Risk Management Process

To integrate risk management throughout an organization, NIST SP 800-39 describes three organizational tiers that address risk and SCRM requires the involvement of all three tiers. [16]

When evaluating supply chain-related risks, it is important to understand that risks must be viewed according to potential scope. This is generally broken down into three (3) tiers of risk:

- Tier 1 – Organization (strategic risk decisions)
- Tier 2 – Business Processes (operational risk decisions)
- Tier 3 – Information Systems & Data (tactical risk decisions)

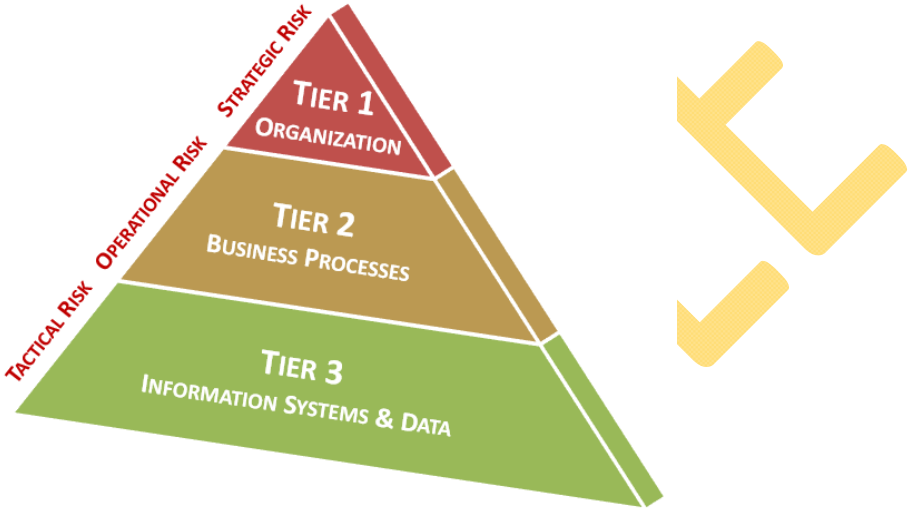

Figure 6. Tiered Risk Model

TIER 1 – ORGANIZATIONAL RISK (STRATEGIC RISK)

Tier 1 provides strategic SCRM direction using organizational-level mission/business requirements and policies, governance structures and organization-wide resource allocation for SCRM. Tier 1 activities help to ensure that SCRM mitigation strategies are cost-effective, efficient and consistent with the strategic goals and objectives of the organization.

Tier 1 SCRM activities include:

- Establishing supporting policies and standards based on applicable statutory, regulatory and contractual obligations.
- Identifying:
  - Mission/business requirements that will influence SCRM, such as cost, schedule, performance, security, privacy, quality and safety;
  - Cybersecurity and data protection requirements, including SCRM-specific requirements; and
  - Organization-wide mission/business functions and how SCRM will be integrated into their processes;
- Establishing risk tolerance level for technology-related supply chain risks;
- Establishing a roles and responsibilities within the organization for SCRM activities; and
- Ensuring that SCRM is appropriately integrated into the organization risk management policies and activities.

TIER 1 GOVERNANCE FUNCTION

Tier 1 stakeholders define corporate strategy, policy, goals and objectives. These stakeholders are executive leadership roles:

- Chief Executive Officer (CEO)
- Chief Operations Officer (COO)
- Chief Financial Officer (CFO)
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Chief Technology Officer (CTO)

[16] NIST SP 800-39 - https://csrc.nist.gov/publications/detail/sp/800-39/final

FEDERAL ACQUISITION REGULATION (FAR) 52.204-21

The ACME Business Consulting, LLC (ACME) Supply Chain Risk Management (SCRM) program requires Third-Party Service Providers (TSP) (e.g., supplier, vendor, contractor, etc.) to implement appropriate technical, administrative and physical controls, regardless of the location or the party responsible for those controls. Implementing and maintain secure practices is a requirement for TSP to do business with ACME and receipt of these requirements serves as notification from ACME to TSP that willful non-compliance with stated requirements may be a violation under the False Claims Act (FCA)[27], so it is imperative that TSP takes its security obligations seriously to avoid any unnecessary legal jeopardy.

ACME is required by US Government regulation to protect regulated data and the systems, applications and services that store, transmit and/or process that regulated data (e.g., Federal Contract Information (FCI)). TSP must protect the confidentiality, integrity, availability and safety of ACME Business Consulting, LLC (ACME) technology assets and data, regardless of how the data is created, distributed or stored. TSP's cybersecurity and data protection controls are expected to be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and system(s), application(s) and service(s), in accordance with all statutory, regulatory and contractual obligations.

TSP's cybersecurity and data protection program must be reasonably designed, implemented and governed to achieve the following objectives:

- As an entity that either (1) has access to regulated data (FCI) and/or (2) stores, transmits and/or processes regulated data (FCI) on behalf of ACME, TSP must address the applicable "flow down" requirements from Federal Acquisition Regulation (FAR) 52.204-21;[28]
- Maintain documented policies, standards and procedures that provide evidence of due care and due diligence in aligning TSP's cybersecurity and data protection program in accordance with its applicable statutory, regulatory and contractual obligations.
- Govern cybersecurity and data protection controls throughout the System Development Life Cycle (SDLC) and information lifecycle to ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of ACME systems, applications, services and data;
- Leverage industry-recognized practices to perform ongoing risk management activities that includes identifying, categorizing and remediating risks;
- Maintain a capability to keep ACME informed of incidents that have the potential to negatively affect ACME's business operations or the CIAS of its technology assets and data; and
- Implement appropriate mechanisms to protect data, systems, applications, services against reasonably-anticipated threats or hazards.

ACME may require a written response that may be an attestation of compliance, a submission of supporting documentation, or both. If ACME requests a written response or request for evidence, TSP is required to submit an electronic copy of the requested documentation. If there are cybersecurity and data protection requirements that are out of scope or that cannot be complied with, TSP must fully explain why the requirement(s) cannot be met with a business justification. Since compensating controls address a control deficiency, if compensating controls are proposed to meet a ACME requirement, ACME must be notified and provided with appropriate context to evaluate the risk associated with the original control not being addressed.

In order to ensure both ACME and TSP are in agreement on the topic of cybersecurity and data protection terminology, ACME recognizes two sources for authoritative definitions and requires TSP to also adopt the same terminology when communicating with ACME:

- The National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Cybersecurity Terms*, is the approved reference document used to define common digital security terms;[29] and
- Unified Compliance Framework (UCF*) Compliance Dictionary*.[30]

[27] False Claims Act Primer - https://www.justice.gov/sites/default/files/civil/legacy/2011/04/22/C-FRAUDS_FCA_Primer.pdf
[28] FAR 52.204-21 - https://www.acquisition.gov/content/52204-21-basic-safeguarding-covered-contractor-information-systems
[29] NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf
[30] UCF Compliance Dictionary - https://compliancedictionary.com