Your Logo
Will Be
Placed Here

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) STRATEGY & IMPLEMENTATION PLAN

CYBERSECURITY & DATA PROTECTION REQUIREMENTS

ACME Business Consulting, LLP

REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

ACME's Information and Communications Technology (**ICT**) and Operational Technology (**OT**) rely on a complex, globally distributed, extensive and interconnected supply chain ecosystem that is comprised of geographically-diverse routes and consists of multiple levels of outsourcing.

ACME's Cybersecurity Supply Chain Risk Management Strategy & Implementation Plan (**C-SCRM SIP**) 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 800-150: *Guide to Cyber Threat Information Sharing*
  - 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 rev 1: *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*
  - ISO 31010: *Risk Management*
- Other References:
  - Center for Internet Security (**CIS**)[3]
  - Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)[4]
  - Cybersecurity Maturity Model Certification (**CMMC**)[5]
  - Fair Information Practice Principles (**FIPP**)[6]
  - MITRE: Deliver Uncompromised: Securing Critical Software Supply Chains[7]
  - MITRE: Standardizing SBOM Within The SW Development Tool Ecosystem[8]
  - National Telecommunications and Information Administration (**NTIA**)[9]
  - Open Web Application Security Project (**OWASP**)[10]
  - Executive Order 14028[11]
  - Secure Controls Framework (**SCF**) [12]

[1] National Institute of Standards and Technology - http://csrc.nist.gov/publications/PubsSPs.html
[2] International Organization for Standardization - https://www.iso.org
[3] Center for Internet Security - https://www.cisecurity.org/
[4] Cloud Security Alliance - https://cloudsecurityalliance.org/
[5] Office of the Under Secretary of Defense for Acquisition & Sustainment - https://www.acq.osd.mil/cmmc/draft.html
[6] Federal Trade Commission - https://www.ftc.gov
[7] MITRE - https://www.mitre.org/publications/technical-papers/deliver-uncompromised-securing-critical-software-supply-chains
[8] MITRE - https://www.mitre.org/publications/technical-papers/standardizing-sbom-within-the-sw-development-tooling-ecosystem
[9] NTIA - https://www.ntia.gov/SBOM
[10] Open Web Application Security Project - https://www.owasp.org/index.php/Main_Page
[11] EO 14028 - https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains
[12] Secure Controls Framework - https://www.securecontrolsframework.com

Table of Contents

This section serves to provide user-oriented guidance that describes critical concepts that drive operations from an integrated systems point of view (e.g., mission, operational objectives and overall expectations).

This document addresses ACME Business Consulting, LLP's (ACME) Strategy & Implementation Plan (**SIP**) for integrating the broad concept of Cybersecurity Supply Chain Risk Management (**C-SCRM**) into discrete risk management activities by applying a multilevel, C-SCRM-specific approach to identify threats and manage the risk associated with ACME's products and services. This includes methodologies to evaluate both technical and non-technical safeguards to determine the effectiveness of implemented cybersecurity and privacy controls.

CAPABILITY NEED

According to the National Counterintelligence Strategy of the United States (years 2020-2022), the strategic objective for supply chain security is to: "*Reduce threats to key U.S. supply chains to prevent foreign attempts to compromise the integrity, trustworthiness and authenticity of products and services purchased and integrated into the operations of the U.S. Government, the Defense Industrial Base and the private sector*."[13]

Cybersecurity Supply Chain Risk Management (**C-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. ACME's Cybersecurity Supply Chain Risk Management Strategy & Implementation Plan (**C-SCRM SIP**) exists to ensure that cybersecurity and privacy-related risks are visible to and understood by the Line of Business (**LOB**) stakeholders who are responsible for the products and/or services involved. The capability exists to expertly advise and educate on C-SCRM matters, while providing oversight to ACME's executive management that is capable of holding the LOB and other key stakeholders accountable for their associated C-SCRM practices.

The C-SCRM SIP prescribes a comprehensive framework for:

- Creating a set of guidelines for C-SCRM practices at ACME;
- Protecting the Confidentiality, Integrity, Availability and Safety (**CIAS**) of ACME's systems, applications, services and data throughout the supply chain;
- Recognizing the diverse supply chain provides both hardware and software components to enable ACME to create its products and services;
- Recognizing the highly-networked nature of the current computing environment that provides ACME-wide governance of cybersecurity and privacy risks; and
- Providing for the development, review and maintenance of the controls required to ensure proactive C-SCRM practices.

PURPOSE

C-SCRM is the organized and purposeful management of cybersecurity risks throughout the supply chain. Therefore, C-SCRM requires enterprise recognition and awareness, since it is a business enabling function that lies at the intersections of the following capabilities:

- Security provides the confidentiality, integrity and availability of:
  - Information that describes the supply chain (e.g., information about the paths of products and services, both logical and physical);
  - Information, products and services that traverse the supply chain (e.g., intellectual property contained in products and services); and/or
  - Information about the parties participating in the supply chain (anyone who touches a product or service throughout its life cycle).
- Suitability is focused on the supply chain and the provided products and services being right and appropriate for the enterprise and its purpose.
- Safety is focused on ensuring that the product or service is free from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property or damage to the environment.
- Reliability is focused on the ability of a product or service to function as defined for a specified period of time in a predictable manner.
- Usability is focused on the extent to which a product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

[13] National Counterintelligence Strategy of the United States of America 2020-2022 - https://www.dni.gov/index.php/ncsc-features/2741-the-national-counterintelligence-strategy-of-the-united-states-of-america-2020-2020

Risk, threat and vulnerability management practices are meant to achieve a minimum level of protection for ACME's business operations. This equates to a reduction in the total risk ACME faces due to the protections offered by implemented cybersecurity and privacy controls. These "risk management ecosystem" components have unique meanings that need to be understood to reasonably protect people, processes, technology and data.

Understanding the context of how these components integrate can lead to more meaningful and practical C-SCRM practices, since Suppliers, Integrators and Service Providers (**SISP**) should be viewed as a potential threat to ACME.

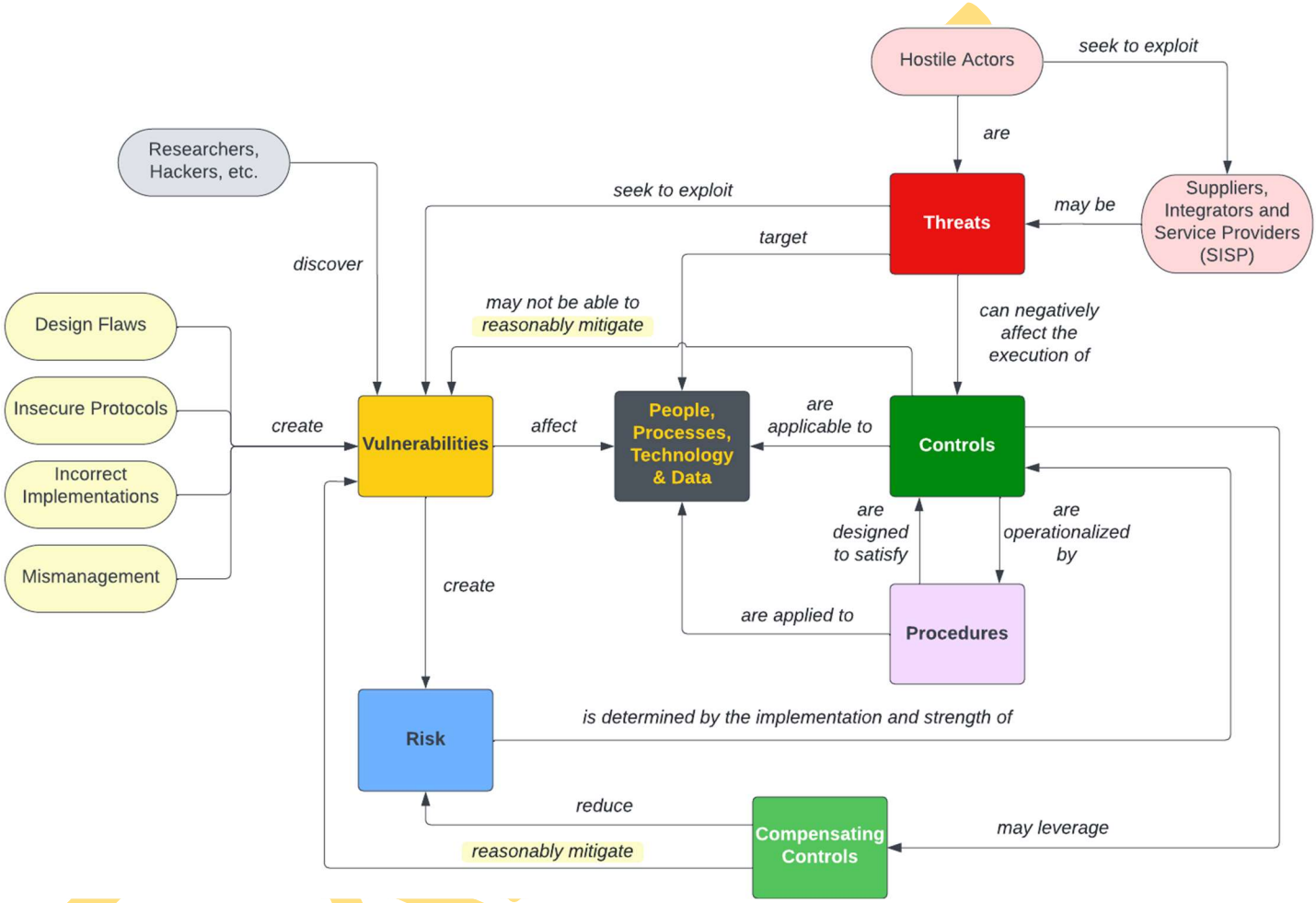

Figure 5. Risk, threat & vulnerability ecosystem

The following contextual definitions help provide clarity about how the terms shown above are to be used:

- **Threat**
  - *noun* A person or thing likely to cause damage or danger.
  - *verb* To indicate impending damage or danger.
- **Risk**
  - *noun* A situation where someone or something valued is exposed to danger, harm or loss.
  - *verb* To expose someone or something valued to danger, harm or loss.
- **Vulnerability**. A weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.
- **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.
- **Compensating Control**. The security controls employed in lieu of the recommended control(s) that provide equivalent or comparable protection for an information system or organization.
- **Procedure**. A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event. The design and implementation of a procedure must be reasonable and appropriate to address the control.

- **Reasonable**. Appropriate or fair level of care. This forms the basis of the legal concepts of "due diligence" and "due care" that pertain to negligence.
- **Mitigate**. The security controls employed in lieu of the recommended control(s) that provide equivalent or comparable protection for an information system or organization.

To integrate risk management throughout an organization and across the supply chain, NIST SP 800-39 and NIST SP 800-161 R1 describe three (3) organizational tiers, or levels, that address risk. [17]

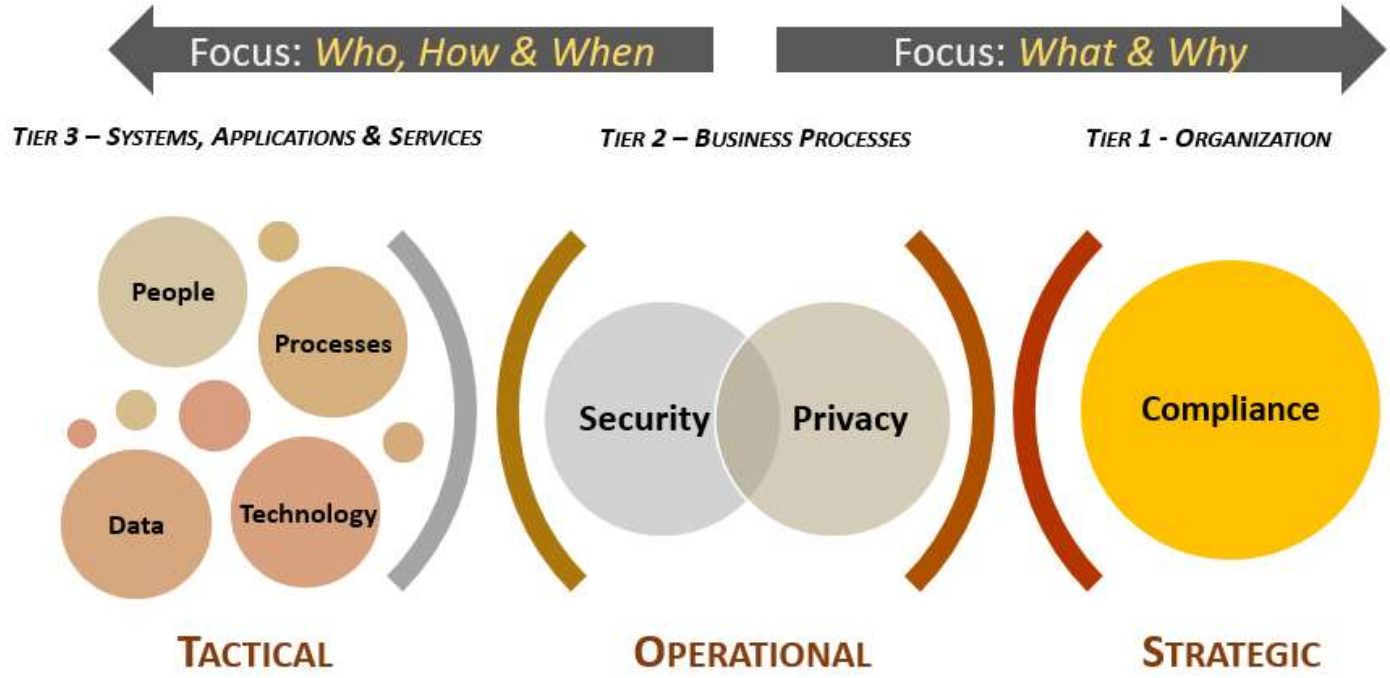

Figure 6. Strategic, operational and tactical C-SCRM considerations

When evaluating supply chain-related risks with Suppliers, Integrators and Service Providers (**SISP**), it is important to understand that risks must be viewed according to potential scope. This is generally broken down into the following risk tiers:

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

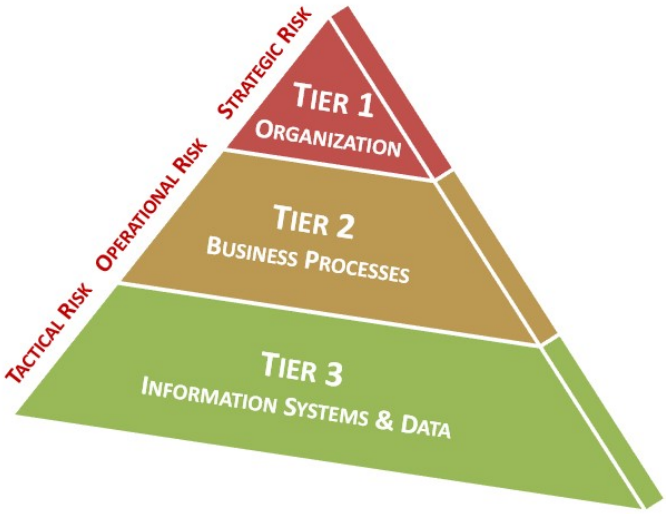

Figure 7. Tiered risk model

[17] NIST SP 800-39 - https://csrc.nist.gov/publications/detail/sp/800-39/final & NIST SP 800-161 R1 - https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

RISK TOLERANCE, RISK THRESHOLD & RISK APPETITE

For ACME's definitive guidance on risk management practices, reference the Risk Management Program (**RMP**).

Controls are the nexus of a cybersecurity and privacy program, so it is vitally important to understand how controls should be viewed from a risk management perspective. To progress from identifying a necessary control to a determination of risk, it is a journey that has several steps, each with its own unique terminology. Therefore, it is important to baseline the understanding risk management terminology. The intent of standardizing risk terminology for categories is so that all ACME personnel can speak the same "risk language" across the enterprise. Categorization also allows management to compare and prioritize risks.

According to the Project Management Body of Knowledge (**PMBOK®**) Guide:[18]

- Risk Tolerance is the "*specified range of acceptable results*."
- Risk Threshold is the "*level of risk exposure above which risks are addressed and below which risks may be accepted*."
- Risk Appetite is the "*degree of uncertainty an organization or individual is willing to accept in anticipation of a reward*." It is important to note that the risk tolerance and risk appetite are not the same thing. In terms of cybersecurity materiality, risk tolerance matters.

On a broad level, risk appetite represents the types and amount of risk that an enterprise is willing to accept in pursuit of value. Conversely, risk tolerance is the enterprise or stakeholder's readiness to bear the remaining risk after a risk response in order to achieve their objectives with the consideration that such tolerance can be influenced by legal or regulatory requirements. This definition is adapted from COSO, which states that risk tolerance is the acceptable level of variation relative to achievement of a specific objective.[19]

Together, risk appetite and risk tolerance provide expectations and acceptable boundaries for performance against ACME's strategic objectives. This figure below illustrates how risk appetite and risk tolerance may be used as guidelines for an organization's operational decision makers. Risk tolerance may be set with boundaries that exceed risk appetite to provide a degree of flexibility for achieving strategic objectives. However, operational decision makers should strive to remain within risk appetite during normal conditions and exceed the boundaries only as absolutely necessary (e.g., to capitalize on significant opportunities, avoid highly adverse conditions). Observed periods of performance in the "Review Zone," which lies outside of risk appetite boundaries, should trigger a review of operational decisions and defined risk appetite and tolerance statements. The review is critical to ensuring that ACME's appetite for risk remains appropriate and applicable given internal and external operating conditions.

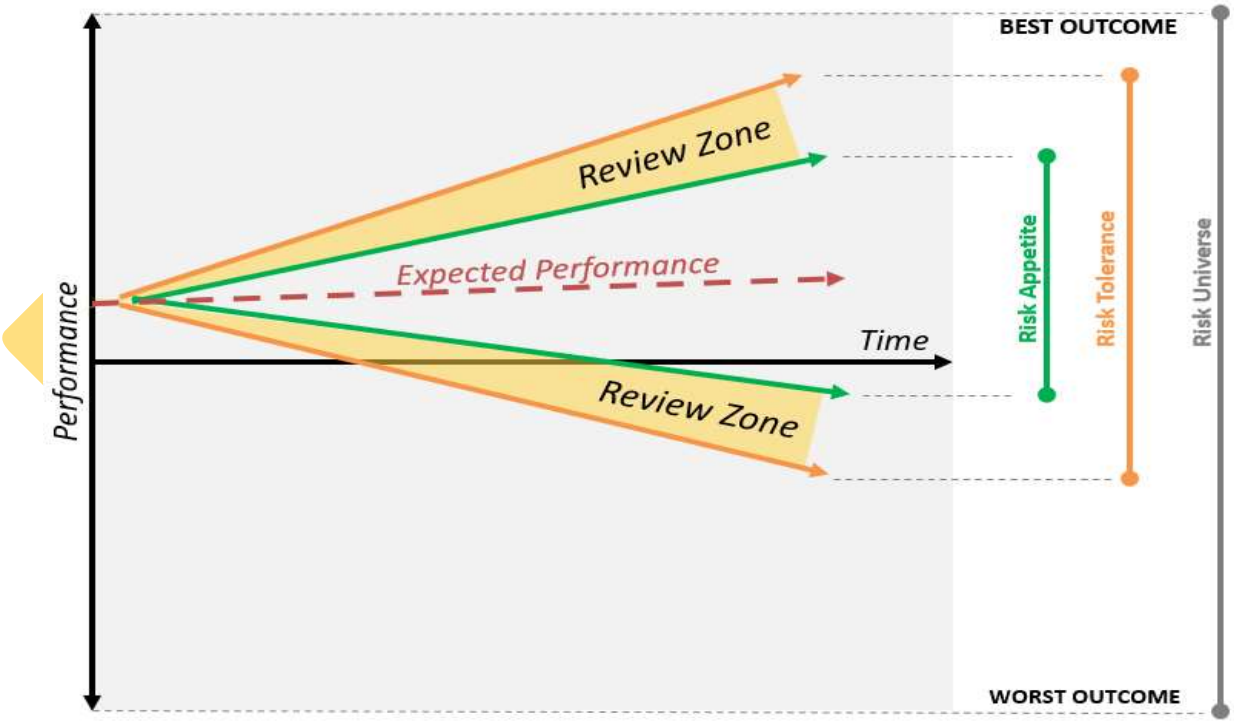

Figure 8. NIST SP 800-161 R1 risk appetite & risk tolerance (G-4)

[18] PMBOK® Guide - https://www.pmi.org/pmbok-guide-standards/foundational/PMBOK
[19] Committee of Sponsoring Organizations of the Treadway Commission (COSO) - https://www.coso.org/

TIER 1 – GOVERNANCE FUNCTION

Tier 1 governance functions sets the tone and direction for enterprise-wide C-SCRM activities by providing an overarching C-SCRM strategy, a C-SCRM policy and a high-Tier implementation plan that shapes how C-SCRM is implemented across ACME.

Within Tier 1:

- Governance structures are formed to enable senior leaders and executives to collaborate on C-SCRM with the risk executive function, make C-SCRM decisions, delegate decisions to Tier 2 and Tier 3;
- Resource allocation is prioritized enterprise-wide for C-SCRM; and
- C-SCRM risk mitigation strategies are developed to be consistent with ACME's strategic goals and objectives.

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 Supply Chain Officer (**CSCO**)
- Chief Information Officer (**CIO**)
- Chief Information Security Officer (**CISO**)
- Chief Technology Officer (**CTO**)
- Chief Financial Officer (**CFO**)

TIER 1 – SISP CONSIDERATIONS

If a SISP claims to govern its technology-related supply chain risks, its Tier 1 governance function should be:

- Integrating C-SCRM considerations into enterprise risk management and continuous monitoring processes;
- Monitoring and evaluating enterprise-level constraints and supply chain risks for change and impact; and
- Monitoring effectiveness of enterprise-level risk response.

Governance "deliverables" from the SISP that should be available to ACME for review include, but are not limited to:

- Documented policies and standards;
- Documented Risk Management Program (**RMP**) that includes C-SCRM considerations;
- Formal risk decisions to avoid, mitigate, share or transfer risk;
- Formal decisions to select, tailor and implement appropriate enterprise C-SCRM controls (e.g., C-SCRM plan); and
- Documented cybersecurity and privacy controls that are specific to C-SCRM.

TIER 1 – THREAT CONSIDERATIONS

From the Threat Catalog in *C-SCRM SIP Supplemental - Annex 4*, Tier 1 threats include, but are not limited to:

- Civil or Political Unrest (MT-1). Civil or political unrest can be singular or wide-spread events that can be unexpected and unpredictable. These events can occur anywhere and at any time, including armed conflict (e.g., war).
- Hacking & Other Cybersecurity Crimes (MT-2). Unlike physical threats that prompt immediate action (e.g., "stop, drop and roll" in the event of a fire), cyber incidents are often difficult to identify as the incident is occurring. Detection generally occurs after the incident has occurred, with the exception of "denial of service" attacks. The spectrum of cybersecurity risks is limitless and threats can have wide-ranging effects on the individual, organizational, geographic and national levels.
- Dysfunctional Management Practices (MT-8). Dysfunctional management practices are a manmade threat that expose an organization to significant risk. The threat stems from the inability of weak, ineffective and/or incompetent management to (1) make a risk-based decision and (2) support that decision. The resulting risk manifests due (1) an absence of a required control or (2) a control deficiency.
- Statutory / Regulatory / Contractual Obligation (MT-11). Laws, regulations and/or contractual obligations that directly or indirectly weaken an organization's security & privacy controls. This includes hostile nation states that leverage statutory and/or regulatory means for economic or political espionage and/or cyberwarfare activities.
- Conflict of Interest (MT-12). Conflict of Interest (COI) is a broad category, but pertains to an ethical incompatibility. COI exist when (1) the concerns or goals of different parties are incompatible or (2) a person in a decision-making position is able to derive personal benefit from actions taken or decisions made in their official capacity.
- Macroeconomics (MT-13). Macroeconomic factors that can negatively affect the global supply chain. Macroeconomic factors directly impact unemployment rates, interest rates, exchange rates and commodity prices. Due to how fiscal and monetary policies can negatively affect the global supply chain, this can disrupt or degrade an organization's business operations.

TIER 1 – RISK CONSIDERATIONS

From the Risk Catalog in *C-SCRM SIP Supplemental - Annex 5*, Tier 1 risks include, but are not limited to:

- Business interruption (R-BC-1)
- Reduction in productivity (R-BC-3)

- Information loss / corruption or system compromise due to technical attack (R-BC-4)
- Information loss / corruption or system compromise due to non-technical attack (R-BC-5)
- Loss of revenue (R-EX-1)
- Cancelled contract (R-EX-2)
- Diminished competitive advantage (R-EX-3)
- Diminished reputation (R-EX-4)
- Fines and judgements (R-EX-5)
- Inability to support business processes (R-GV-1)
- Inadequate internal practices (R-GV-4)
- Inadequate third-party practices (R-GV-5)
- Lack of oversight of internal controls (R-GV-6)
- Lack of oversight of third-party controls (R-GV-7)
- Expense associated with managing a loss event (R-IR-4)
- Inability to maintain situational awareness (R-SA-1)

TIER 1 – C-SCRM ASSESSMENT CONSIDERATIONS

At a minimum, the following high-level criteria should be assessed to determine Tier 1 risks posed to ACME:

- Examine the legitimacy / ownership of supply chain entities for evidence of a shell company or undue influence from another company or foreign government;
- Examine organizational supply chain information including that from supply chain maps to identify especially vulnerable locations or organizations;
- Analyze organizational mission for susceptibility to potential supply chain vulnerabilities;
- Examine system integrator and supplier relationships for susceptibility to potential supply chain vulnerabilities; and
- Review enterprise architecture and criticality baseline to identify areas of weakness requiring more robust supply chain considerations.

The assessment of Tier 1 risks should be viewed from applicable ACME technology and business constraints:

- ACME's mission, strategy, policies and governance structure;
- Applicable laws and regulations;
- Mission functions; and
- Existing processes (e.g., security, quality, etc.).

TIER 2 – BUSINESS PROCESS RISK (OPERATIONAL RISK)

Tier 2 addresses risk from a business process perspective and is informed by the risk context, risk decisions and risk activities at Tier 1. In Tier 2, program requirements are defined and managed, including cost, schedule, performance and a variety of critical nonfunctional requirements. These nonfunctional requirements include concepts such as reliability, dependability, safety, security and quality. Many threats to and by the supply chain are addressed at this level by the mismanagement of trust relationships between system integrators, suppliers and external service providers of technology-related products and services. Since C-SCRM can both directly and indirectly impact ACME's business processes, it is critical to understand, integrate and coordinate C-SCRM activities at this tier to ensure successful business operations and overall mission accomplishment.

Tier 2 C-SCRM activities include:

- Defining the risk response strategy, including C-SCRM considerations, for critical processes;
- Establishing C-SCRM processes to support business processes;
- Determining the C-SCRM requirements of the business systems needed to execute the business processes;
- Incorporating C-SCRM requirements into existing business processes;
- Documenting provenance;
- Integrating C-SCRM requirements into an enterprise architecture to facilitate the allocation of C-SCRM controls to organizational information systems and the environments in which those systems operate; and
- Establishing a Line of Business (**LOB**)-specific C-SCRM team that coordinates and collaborates with ACME's centralized C-SCRM team.

TIER 2 – GOVERNANCE FUNCTION

Tier 2 stakeholders identify additional sources of threat information specific to organizational mission functions. These stakeholders are generally mid-level management roles:

- Program / project management;
- IT / cybersecurity management;

For C-SCRM SIP to be successful, operational leadership is essential. This requires "active participation" by a Chief Supply Chain Officer (**CSCO**) (commonly referred to as a Chief Operating Officer (**COO**)) and the CSCO's designated representatives, ensures that processes are effectively carried out on a day-to-day basis.

For the CSCO role to be successful in executing the organization's C-SCRM SIP:

- The CSCO needs to report directly to the organization's Chief Executive Officer (**CEO**) to eliminate conflicts of interests among leadership representing LOB within ACME.
- The CSCO must be able to influence cybersecurity and privacy controls by being part of the organization's cybersecurity steering committee.
- Due to the reliance on risk management practices and the underlying cybersecurity and privacy controls that enable a C-SCRM SIP to function, the Chief Information Security Officer (**CISO**) should directly report to the CSCO.
- Due to the supply chain nature of DevSecOps, the Chief Technology Officer (**CTO**) role should directly report to the CSCO.
- Due to the external focus of the C-SCRM SIP, the Chief Contracting Officer (**CCO**) role should directly report to the CSCO to ensure contracts and procurement actions are in-line with the C-SCRM SIP.
- Due to how technology is so integral to business operations, the Chief Information Officer (**CIO**) role should directly report to the CSCO.
- The CISO, CIO, CTO and CCO need to be viewed as peers, each with an equal role of importance in the C-SCRM SIP, where the CSCO provides operational leadership to orchestrate C-SCRM activities across the enterprise and its supply chain.

For the reasons stated above, it demonstrates how "executive management buy-in" is essential for the overall C-SCRM SIP to function appropriately. This involves "messaging from the top" at the Board of Directors (**BoD**) and CEO levels, so that corporate executives (**CxO**) will be forced to adopt the practices within their Lines of Business (**LOB**) to address their inherent risks with technology and the supply chain.

C-SCRM is a multi-player effort, so ACME must adopt a "*One Team! One Fight!*" mentality that is first and foremost driven by ACME's executive leadership team. Additionally, the organization's Internal Audit (**IA**) function plays a crucial role in maintaining internal accountability, where there is a neutral system of checks and balances to ensure C-SCRM practices are operational and risk is kept within ACME's acceptable risk threshold.

C-SCRM PROGRAM STAKEHOLDERS

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

- Secure Development Practices
- Procurement Practices
- Risk Management Practices
- 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.[21]

[21] 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

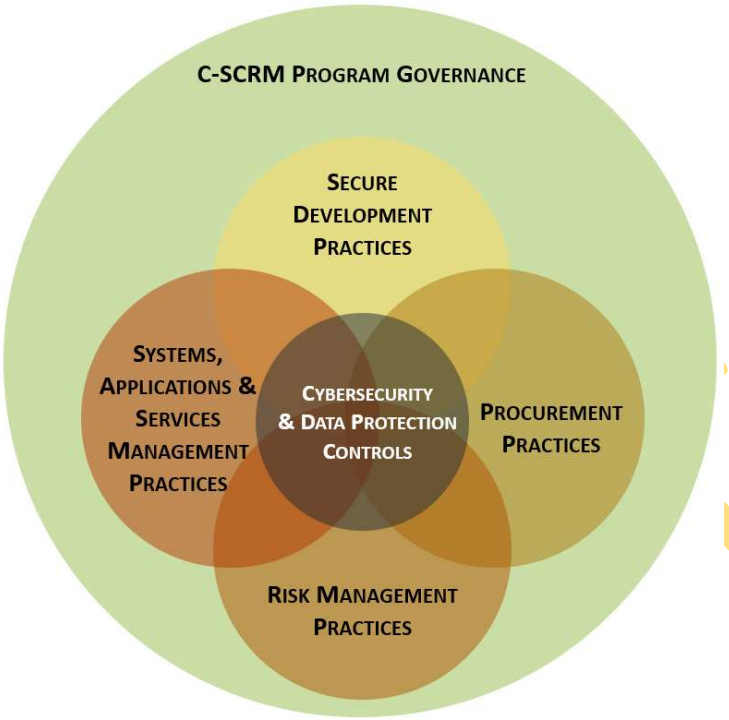

Figure 12. C-SCRM Organizational Components

Secure Development Practices

C-SCRM is an enterprise-wide activity that is implemented throughout the System Development Life Cycle (**SDLC**). 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.

Procurement Practices

C-SCRM lies at the intersection of cybersecurity and supply chain risk management. Existing supply chain and cybersecurity practices provide a foundation for building an effective Risk Management Program (**RMP**). Therefore, within the concept of procurement practices, in order to ensure C-SCRM is operational it takes the following to exist and be functional:

- Increased executive leadership or Board of Directors (**BoD**) involvement for establishing C-SCRM as a top business priority and to ensure proper oversight.
- C-SCRM intersects with the BoD fiduciary "duty of care" and BoD-level training should be provided to board members understand the current state and weaknesses of the organization's supply chain, including the BoD's responsibilities in executing a C-SCRM strategy.
- Clear governance of C-SCRM activities that includes cross-organizational roles and responsibilities with clear definitions and designation/distribution of these roles among enterprise risk management, supply chain, cybersecurity, product management and product security (if applicable) and other relevant functions appropriate for the organization's business.

C-SCRM Practice Implementation

Cybersecurity supply chain risk management builds on existing standardized practices in multiple disciplines and an ever-evolving set of C-SCRM capabilities:

- Foundational;
- Sustaining; and
- Enhancing.

Foundational Practices

Having foundational practices in place is critical to successfully and productively interacting with Suppliers, Integrators and Service Providers (**SISP**).

[edit as necessary – the following are specific examples of the recommended multidisciplinary foundational practices that can be incrementally implemented to improve an enterprise's ability to develop and execute more advanced C-SCRM practices]

- Establish a core, dedicated, multidisciplinary C-SCRM Program Management Office and/or C-SCRM team.
- Obtain senior leadership support for establishing and/or enhancing C-SCRM.
- 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 enterprise-wide risk assessment process (in accordance with NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments [NIST SP 800-30 Rev. 1]).
- Establish an enterprise governance structure that integrates C-SCRM requirements and incorporates these requirements into the enterprise policies.
- Develop a process for identifying and measuring the criticality of the enterprise'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. Supervisors and managers should also ensure that their staff aims to build C-SCRM competencies.
- 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, physical security and other relevant processes (e.g., Legal, Risk Executive, HR, Finance, Enterprise IT, Program Management/System Engineering, Information Security, Acquisition/Procurement, Supply Chain Logistics, etc.).
- Ensure that adequate resources are dedicated and allocated to information security and C-SCRM to ensure proper implementation of policy, guidance and controls.
- Ensure sufficient cleared personnel with key C-SCRM roles and responsibilities to access and share C-SCRM-related classified information.
- Implement an appropriate and tailored set of baseline information security controls found in NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Enterprises [NIST SP 800-53, Rev. 5].
- Establish internal checks and balances to ensure compliance with security and quality requirements.
- Establish a supplier management program that includes, for example, guidelines for purchasing from qualified original equipment manufacturers (**OEMs**) or their authorized distributors and resellers.
- Implement a robust incident management program to successfully identify, respond to and mitigate security incidents. This program should be capable of identifying the root cause of security incidents, including those that originate from the cybersecurity supply chain.
- Establish internal processes to validate that suppliers and service providers actively identify and disclose vulnerabilities in their products.
- Establish a governance capability for managing and monitoring components of embedded software to manage risk across the enterprise (e.g., SBOMs paired with criticality, vulnerability, threat and exploitability to make this more automated).

Sustaining Practices

Sustaining practices should be used to enhance the efficacy of cybersecurity supply chain risk management capabilities. These practices are inclusive of and build upon foundational practices. When ACME has broadly standardized and implemented the foundational practices, these are the next steps in advancing ACME's C-SCRM capabilities:

C-SCRM Requirements by Geographic Region

The following matrixes are arranged by geographic reason to identify applicable:

- Corruption Practices Index *[as of 2021]*; [34]
- Data Localization Laws;
- Geographic-specific Intellectual Property (**IP**) threats (e.g., 301 Report Priority Watch List & Watch List) *[as of 2022]*;[35]
- Designated State Sponsors of Terrorism (**DSST**) *[as of 2022]*;[36]
- Notorious Markets List (**NML**) *[as of 2021]*;[37] and
- Export Administration Regulation (**EAR**) *[as of 2 June 2022]*[38]
    - D:1 – National Security
    - D:2 – Nuclear
    - D:3 – Chemical & Biological
    - D:4 – Missile Technology
    - D:5 – U.S. Arms Embargo
    - E:1 – Terrorist Supporting Countries
    - E:2 – Unilateral Embargo

The C-SCRM SIP is architected to empower management at the lowest level, where four (4) tiers exist that allow for escalation. These tiers provide ACME with the appropriate level of management oversight, based on the level of risk:

- Level 1: Line Management
- Level 2: Senior Management
- Level 3: Executive Management
- Level 4: Board of Directors

AMER: North, Central & South America

The following matrix covers the AMER region that addresses North, Central and South American countries:

Country	CPI	Data Localization	301 Report		DSST	NML	EAR							Risk Management Tier Approval & Prohibition Considerations
			Priority Watch List	Watch List			D:1	D:2	D:3	D:4	D:5	E:1	E:2	
Anguilla	N/A													
Antigua and Barbuda	N/A													
Argentina	38		X			X								Level 2 (Senior Management) review: IP risk | high corruption risk
Aruba	N/A													
Bahamas	64													Level 1 (Line Management) review: moderate corruption risk
Barbados	65			X										Level 2 (Senior Management) review: IP risk | moderate corruption risk
Belize	N/A													
Bermuda	N/A													

[34] Corruption Perceptions Index - https://www.transparency.org/en/cpi/2021/index/cod
[35] 301 Report - https://ustr.gov/issue-areas/intellectual-property/special-301
[36] DSST - https://www.state.gov/state-sponsors-of-terrorism/
[37] NML - https://ustr.gov/sites/default/files/IssueAreas/IP/2021%20Notorious%20Markets%20List.pdf
[38] EAR - https://www.bis.doc.gov/index.php/documents/regulation-docs/2255-supplement-no-1-to-part-740-country-groups-1/file

Bolivia	30			X										Level 2 (Senior Management) review: IP risk | high corruption risk
Bonaire, Sint Eustatius and Saba	N/A													
Bouvet Island	N/A													
Brazil	38			X		X								Level 2 (Senior Management) review: IP risk | high corruption risk
British Virgin Islands	N/A													
Canada	74			X		X								Level 2 (Senior Management) review: IP risk
Cayman Islands	N/A													
Chile	67		X											Level 2 (Senior Management) review: IP risk | moderate corruption risk
Colombia	39			X										Level 2 (Senior Management) review: IP risk | high corruption risk
Costa Rica	58													Level 1 (Line Management) review: moderate corruption risk
Cuba	46				X			X	X		X		X	Level 4 (Board of Directors) review: prohibited country | high corruption risk
Curaçao	N/A													
Dominica	55													Level 1 (Line Management) review: moderate corruption risk
Dominican Republic	30			X										Level 2 (Senior Management) review: IP risk | high corruption risk
Ecuador	36			X										Level 2 (Senior Management) review: IP risk | high corruption risk
El Salvador	34													Level 2 (Senior Management) review: high corruption risk
Falkland Islands (Malvinas)	N/A													
French Guiana	N/A													
Grenada	53													Level 1 (Line Management) review: moderate corruption risk
Guadeloupe	N/A													
Guatemala	25			X										Level 2 (Senior Management) review: IP risk | high corruption risk

- SUPPLEMENTAL DOCUMENTATION -

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) STRATEGY & IMPLEMENTATION PLAN

ANNEXES, TEMPLATES & REFERENCES

Version 2022.1

TABLE OF CONTENTS

ANNEX 3: BASELINE SECURITY CATEGORIZATION GUIDELINES

Assets and services are categorized by two primary attributes: (a) the potential impact they pose from misuse and (b) the data classification level of the data processed, stored or transmitted by the asset or process. These two attributes combine to establish a basis for controls that should be assigned to that system or asset. *This basis is called an Assurance Level (AL).*

DATA SENSITIVITY

This is straightforward where the data sensitivity rating represents the highest data classification of the data processed, stored or transmitted by the asset or process

SAFETY & CRITICALITY

The Safety & Criticality (SC) rating reflects two aspects of the "importance" of the asset or process:

- On one hand, SC simply represents the importance of the asset relative to the achievement of the company's goals and objectives (e.g., business critical, mission critical, or non-critical).
- On the other hand, SC represents the potential for harm that misuse of the asset or service could cause to ACME, its clients, its partners, or the general public.

The three (3) SC ratings are:

- SC-1: Mission Critical. This category involves systems, services and data that is determined to be vital to the operations or mission effectiveness of ACME:
  - Includes systems, services or data with the potential to significantly impact the brand, revenue or customers.
  - Any business interruption would have a significant impact on ACME's mission.
    - Cannot go down without having a significant impact on ACME's mission.
    - The consequences of loss of integrity or availability of a SC-1 system are unacceptable and could include the immediate and sustained loss of mission effectiveness.
  - *Requires the most stringent protection measures that exceed leading practices* to ensure adequate security.
  - Safety aspects of SC-1 systems, services and data could lead to:
    - Catastrophic hardware failure;
    - Unauthorized physical access to premises; and/or
    - Physical injury to users.
- SC-2: Business Critical. This category involves systems, services and data that are determined to be important to the support of ACME's business operations:
  - Includes systems, services or data with the potential to moderately impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to twenty-four (24) hours (e.g., one (1) business day) without having a significant impact on ACME's mission.
    - Loss of availability is difficult to deal with and can only be tolerated for a short time.
    - The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or the ability to operate.
    - The consequences of loss of integrity are unacceptable.
  - *Requires protection measures equal to or beyond leading practices* to ensure adequate security.
  - Safety aspects of SC-2 systems could lead to:
    - Loss of privacy; and/or
    - Unwanted harassment.
- SC-3: Non-Critical. This category involves systems, services and data that are necessary for the conduct of day-to-day operations, but are not business critical in the short-term:
  - Includes systems, services or data with little or potential to impact the brand, revenue or customers.
  - Affected systems, services or data can go down for up to seventy-two (72) hours (e.g., three (3) business days) without having a significant impact on ACME's mission.
    - The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness.
    - The consequences could include the delay or degradation of services or routine activities.
  - *Requires protection measures that are commensurate with leading practices* to ensure adequate security.
  - Safety aspects of SC-3 systems could lead to:
    - Inconvenience;
    - Frustration; and/or
    - Embarrassment.

Where the data sensitivity and SC levels meet are considered the Assurance Levels (AL). The AL represents the "level of effort" that is needed to properly ensure the Confidentiality, Integrity, Availability and Safety (CIAS) of the asset or process.

Asset Categorization Matrix		Data Sensitivity			
		RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Safety & Criticality	SC-1 Mission Critical	Enhanced	Enhanced	Enhanced	Enhanced
	SC-2 Business Critical	Enhanced	Enhanced	Basic	Basic
	SC-3 Non-Critical	Enhanced	Basic	Basic	Basic

Figure 1: Asset Categorization Risk Matrix

Basic Assurance Requirements

- The minimum level of controls is defined as industry-recognized leading practices (e.g., PCI DSS, NIST SP 800-53, ISO 27002, etc.).
- For security controls in Basic assurance projects or initiatives, the focus is on the digital security controls being in place with the expectation that no obvious errors exist and that as flaws are discovered they are addressed in a timely manner.

Enhanced Assurance Requirements

- The minimum level of controls is defined as exceeding industry-recognized leading practices (e.g., DLP, FIM, DAM, etc.).
- For security controls in Enhanced Assurance projects, it is essentially the Standard Assurance level that is expanded to require more robust Cybersecurity capabilities that are commensurate with the value of the project to ACME.

ANNEX 4: THREAT CATALOG

It is necessary to develop a threat catalog that identifies possible natural and man-made threats that affect the entity's security & privacy controls. The use case for the threat catalog is to identify applicable natural and man-made threats that affect control execution. (*e.g., if the threat materializes, will the control function as expected?*) In the context of the SP-RMM, "threat" is defined as:

> *noun A person or thing likely to cause damage or danger.*
> *verb To indicate impending damage or danger.*

This threat catalog is sorted by natural and man-made threats:

NATURAL THREATS

Natural threats are caused by environmental phenomena that have the potential to impact individuals, processes, organizations or society, as a whole. The SP-RMM leverages a catalog of fourteen (14) natural threats:

Threat #	Threat	Threat Description
NT-1	Drought & Water Shortage	Regardless of geographic location, periods of reduced rainfall are expected. For non-agricultural industries, drought may not be impactful to operations until it reaches the extent of water rationing.
NT-2	Earthquakes	Earthquakes are sudden rolling or shaking events caused by movement under the earth's surface. Although earthquakes usually last less than one minute, the scope of devastation can be widespread and have long-lasting impact.
NT-3	Fire & Wildfires	Regardless of geographic location or even building material, fire is a concern for every business. When thinking of a fire in a building, envision a total loss to all technology hardware, including backup tapes and all paper files being consumed in the fire.
NT-4	Floods	Flooding is the most common of natural hazards and requires an understanding of the local environment, including floodplains and the frequency of flooding events. Location of critical technologies should be considered (e.g., server room is in the basement or first floor of the facility).
NT-5	Hurricanes & Tropical Storms	Hurricanes and tropical storms are among the most powerful natural disasters because of their size and destructive potential. In addition to high winds, regional flooding and infrastructure damage should be considered when assessing hurricanes and tropical storms.
NT-6	Landslides & Debris Flow	Landslides occur throughout the world and can be caused by a variety of factors including earthquakes, storms, volcanic eruptions, fire and by human modification of land. Landslides can occur quickly, often with little notice. Location of critical technologies should be considered (e.g., server room is in the basement or first floor of the facility).
NT-7	Pandemic (Disease) Outbreaks	Due to the wide variety of possible scenarios, consideration should be given both to the magnitude of what can reasonably happen during a pandemic outbreak (e.g., COVID-19, Influenza, SARS, Ebola, etc.) and what actions the business can be taken to help lessen the impact of a pandemic on operations.
NT-8	Severe Weather	Severe weather is a broad category of meteorological events that include events that range from damaging winds to hail.

NT-9	Space Weather	Space weather includes natural events in space that can affect the near-earth environment and satellites. Most commonly, this is associated with solar flares from the Sun, so an understanding of how solar flares may impact the business is of critical importance in assessing this threat.
NT-10	Thunderstorms & Lightning	Thunderstorms are most prevalent in the spring and summer months and generally occur during the afternoon and evening hours, but they can occur year-round and at all hours. Many hazardous weather events are associated with thunderstorms. Under the right conditions, rainfall from thunderstorms causes flash flooding and lightning is responsible for equipment damage, fires and fatalities.
NT-11	Tornadoes	Tornadoes occur in many parts of the world, including the US, Australia, Europe, Africa, Asia and South America. Tornadoes can happen at any time of year and occur at any time of day or night, but most tornadoes occur between 4–9 p.m. Tornadoes (with winds up to about 300 mph) can destroy all but the best-built man-made structures.
NT-12	Tsunamis	All tsunamis are potentially dangerous, even though they may not damage every coastline they strike. A tsunami can strike anywhere along most of the US coastline. The most destructive tsunamis have occurred along the coasts of California, Oregon, Washington, Alaska and Hawaii.
NT-13	Volcanoes	While volcanoes are geographically fixed objects, volcanic fallout can have significant downwind impacts for thousands of miles. Far outside of the blast zone, volcanoes can significantly damage or degrade transportation systems and also cause electrical grids to fail.
NT-14	Winter Storms & Extreme Cold	Winter storms is a broad category of meteorological events that include events that range from ice storms, to heavy snowfall, to unseasonably (e.g., record breaking) cold temperatures. Winter storms can significantly impact business operations and transportation systems over a wide geographic region.

Figure 4-1. Natural threats

MANMADE THREATS

Manmade threats are caused by an element of human intent, negligence or error or threat of violence that have the potential to impact individuals, processes, organizations or society, as a whole. The SP-RMM leverages a catalog of thirteen (13) manmade threats:

Threat #	Threat	Threat Description
MT-1	Civil or Political Unrest	Civil or political unrest can be singular or wide-spread events that can be unexpected and unpredictable. These events can occur anywhere, at any time.
MT-2	Hacking & Other Cybersecurity Crimes	Unlike physical threats that prompt immediate action (e.g., "stop, drop and roll" in the event of a fire), cyber incidents are often difficult to identify as the incident is occurring. Detection generally occurs after the incident has occurred, with the exception of "denial of service" attacks. The spectrum of cybersecurity risks is limitless and threats can have wide-ranging effects on the individual, organizational, geographic and national levels.
MT-3	Hazardous Materials Emergencies	Hazardous materials emergencies are focused on accidental disasters that occur in industrialized nations. These incidents can range from industrial chemical spills to groundwater contamination.
MT-4	Nuclear, Biological and Chemical (NBC) Weapons	The use of NBC weapons are in the possible arsenals of international terrorists and it must be a consideration. Terrorist use of a “dirty bomb” — is considered far more likely than use of a traditional nuclear explosive device. This may be a combination a conventional explosive device with radioactive / chemical / biological material and be designed to scatter lethal and sub-lethal amounts of material over a wide area.

ANNEX 6: GENERIC "BEST PRACTICES" CONTRACT ADDENDUMS - FRAMEWORK-SPECIFIC CONTROLS

This annex provides context to add in contracts with Suppliers, Integrators and Service Providers (SISP). The following examples contain text that may be applicable for flow-down requirements to a SISP, based on what is specifically applicable to the SISP due to business and technology considerations:

**** WARNING ** REVIEW WITH LEGAL COUNSEL FOR APPLICABILITY – DO NOT JUST "CUT & PASTE" ** WARNING ****

ISO 27001/27002

The ACME Business Consulting, LLP (ACME) Cybersecurity Supply Chain Risk Management Strategy & Implementation Plan (C-SCRM SIP) program requires Suppliers, Integrators and Service Providers (SISP) (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 SISP to do business with ACME.

SISP must protect the confidentiality, integrity, availability and safety of ACME technology assets and data, regardless of how the data is created, distributed or stored. SISP's cybersecurity and privacy 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.

In order to ensure both ACME and SISP are in agreement on the topic of cybersecurity and privacy terminology, ACME recognizes two sources for authoritative definitions and requires SISP 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;[1] and
- Unified Compliance Framework (UCF*) Compliance Dictionary*.[2]

SISP's cybersecurity and privacy program must be reasonably designed, implemented and governed to achieve the following objectives:

- Demonstrate alignment with ISO/ IEC 27001[3] by implementing an ISO-based Information Security Management System (ISMS);
- Implement cybersecurity and privacy controls from ISO/IEC 27002[4] to support the ISMS;
- Maintain documented policies, standards and procedures that provide evidence of due care and due diligence in aligning SISP's cybersecurity and privacy program in accordance with ISO/IEC 27001 and ISO/IEC 277002.
- Provide an annual report that attests SISP's alignment with ISO/IEC 27001 that includes a report on applicable cybersecurity and privacy deficiencies, including planned steps to remediate deficiencies;
- Govern cybersecurity and privacy 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, SISP is required to submit an electronic copy of the requested documentation. If there are cybersecurity and privacy requirements that are out of scope or that cannot be complied with, SISP 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.

[1] NIST IR 7298 - https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf
[2] UCF Compliance Dictionary - https://compliancedictionary.com
[3] ISO/IEC 27001 - https://www.iso.org/isoiec-27001-information-security.html
[4] ISO/IEC 27002 - https://www.iso.org/standard/54533.html