THIRD-PARTY RISK MANAGEMENT (TPRM) PROGRAM

ACME Consulting Services, LLP

Table of Contents

The purpose of the Third-Party Risk Management (TPRM) policy is to govern Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.

This policy is designed to establish processes that will help ensure cybersecurity & data privacy risks associated with third-parties are minimized or avoided, including if a third-party should become compromised, untrustworthy or defunct.

Third-Party Risk Management (TPRM) Policy: ACME shall implement and maintain industry-recognized Third-Party Risk Management practices to strengthen the security, compliance and resilience of its Third-Party Service Provider (TSPS) ecosystem. ACME's approach to TPRM requires transparency, so third-party provider inventories and risk assessments shall be generated to understand risks associated with dependencies, conflicts of interest, security practices and criticality considerations.

As technologies and processes evolve over time, ACME shall ensure the appropriate levels of due diligence and due care are applied to validate that necessary cybersecurity & data protection controls exist and are effective to govern TPSPs. Through sound procurement and contract management practices, ACME shall cultivate a secure, compliant and resilient TPSP ecosystem that supports ACME's business operations.

SCOPE & APPLICABILITY

These policies, standards and guidelines apply to all ACME data, systems, activities and assets owned, leased, controlled or used by ACME, its agents, contractors or other business partners on behalf of ACME. These policies, standards and guidelines apply to all ACME employees, contractors, sub-contractors and their respective facilities supporting ACME business operations, wherever ACME data is stored or processed, including any third-party contracted by ACME to handle, process, transmit, store or dispose of ACME data.

VIOLATIONS OF POLICIES, STANDARDS AND/OR PROCEDURES

Any ACME user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

EXCEPTION TO STANDARDS

While every exception to a standard potentially weakens protection mechanisms for ACME systems and underlying data, occasionally exceptions will exist. When requesting an exception to ACME's defined TPRM practices, ACME personnel must submit a business justification for deviation from the standard in question.

UPDATES TO POLICIES & STANDARDS

Updates to the TPRM policy will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, procedures, standards and guidelines.

THIRD-PARTY RISK STAKEHOLDERS & DECISION AUTHORITIES

TPRM is far more than a "technology issue" where it requires the direct involvement of business process owners, Information Technology (IT) and cybersecurity functions. Each has a unique role to play in TPRM:

Business Unit

- The Business Unit (BU) that requires a technology-enabled system, application or service ultimately "owns" the risk associated with the ongoing operation of that capability.
- Business Process Owners (BPOs) are individuals within BUs who are the central point of contact for IT and cybersecurity to work with on risk management decisions.

Information Technology (IT)

- IT has a shared responsibility with the BUs to securely operate and maintain systems.
- IT executes vulnerability management tasks.

Cybersecurity

- Cybersecurity operates as a facilitator of risk/threat identification and analysis.
- Cybersecurity focuses on providing expert guidance and support to both IT and the BU.

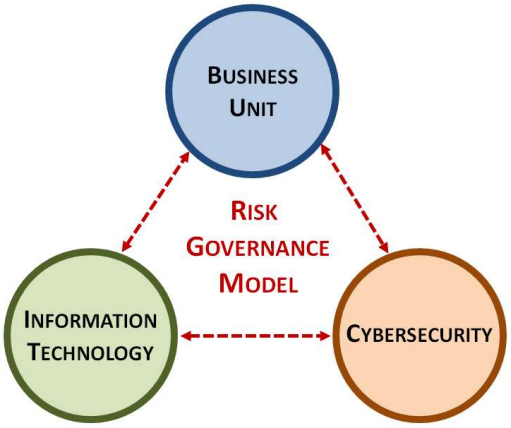

Figure 3. Risk Governance Model

THIRD-PARTY RISK MANAGEMENT (TPRM) LIFECYCLE

To be effective, TPRM must follow a standardized methodology. It is also important to recognize that there is a lifecycle associated with Third-Party Service Provider (TPSP) relationships that consists of the following five (5) stages:

1. Identification;
2. Due Diligence:
    a. Selection Criteria;
    b. Evaluation / Risk Assessment; and
    c. Risk Mitigation.
3. Procurement;
4. Due Care:
    a. Record Keeping and Reporting; and
    b. Ongoing Monitoring; and
5. Offboarding.

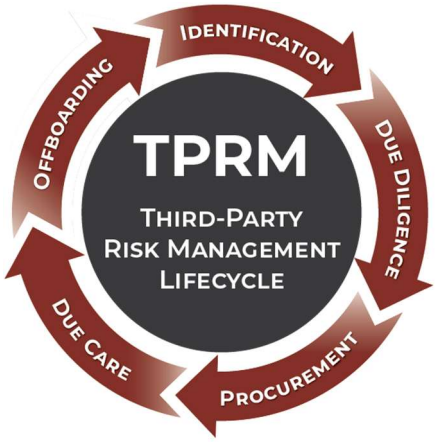

Figure 4. TPRM Lifecycle

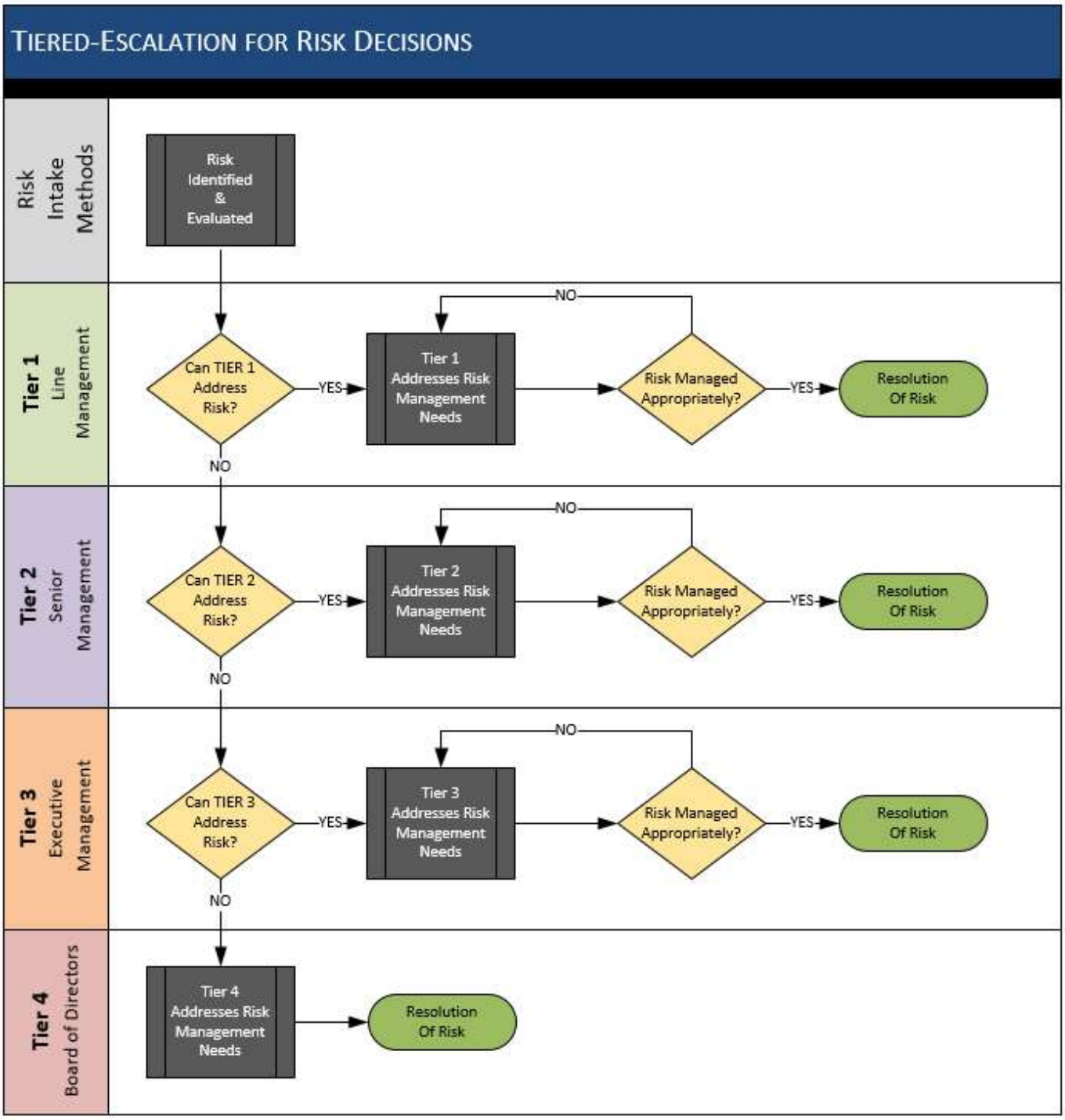

Figure 5. TPRM decision authority tiers

The intent of a tiered approach is for a repeatable, scalable process that manages risk at the lowest possible level of management. Once the risk is identified and evaluated, the appropriate level of management will be required to decide upon the most appropriate risk treatment option.

The process of identifying Third-Party Service Providers (TPSP) is a dynamic process:

- For existing TPSPs, ACME may:
  - Utilize existing contracts to identify TPSPs currently in use; and
- For new TPSPs, ACME may:
  - Take suggestions from its employees for possible candidates to address a business and/or technical need; or
  - Issue a Request For Proposal (RFP) to encourage TPSPs to self-identify interest in working with ACME

TPRM PHASE 1(A): CENTRALIZED INVENTORY

ACME's procurement team is responsible for maintaining a current and accurate inventory of TPSPs. Personnel from ACME's cybersecurity, IT and legal functions will assist the procurement team in properly categorizing the TPSP, based on the risk is presents to ACME, defined as:

(1) Low;
(2) Moderate;
(3) High;
(4) Severe; or
(5) Extreme.

See Appendix B: Risk Categorization for more information on ACME's defined risk categories.

At a minimum, ACME's TPSP inventory must contain the following criteria:

- Formal name of the TPSP;
- Doing Business As (DBA) of the TPSP, if applicable;
- A description of the product(s) and/or service(s) provided by the TPSP;
- The Point of Contact (POC) at ACME responsible for overseeing the delivery of the product(s) and/or service(s), including ACME department / Business Unit (BU);
- ACME employee who authorized the use of the TPRM (e.g., person responsible for accepting the risk associated with the TPRM);
- Identification if the TPSP will have either direct or indirect access to ACME's (includes both logical and physical access):
  - Systems, applications and/or services; and/or
  - Sensitive and/or regulated data;
- Geographic location(s) where the product(s) and/or service(s) will be used;
- Active duration of the contract including:
  - Start date; and
  - End date.
- At least two (2) points of contact at the TPSP that can address TPRM-related questions, including:
  - Email address(es); and
  - Phone number(s);

TPRM PHASE 1(B): EVALUATION CRITERIA

ACME will maintain one (1), or more, defined control sets that are specific to TPRM due diligence activities. See Appendix C: TPRM Cybersecurity & Data Protection Controls for more information on ACME's defined TPRM controls.

In addition to cybersecurity and data protection controls, ACME must evaluate the following TPSP practices:

(1) Adhere to the US National Defense Authorization Act (NDAA) Section 889, *Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment*,[11] and US Federal Acquisition Regulation (FAR)

[11] *NDAA Section 889 - https://www.acquisition.gov/Section-889-Policies*

TPRM Phase 2: Due Diligence

Upon the identification of a TPSP, the next phase in TPRM is for ACME to perform due diligence activities to ensure the TPSP has reasonable cybersecurity and data protection practices in place.

As part of the identification process, ACME's procurement department should identify primary and secondary Points of Contact (POC) for each TPSP, including:

- Direct contact information for specific individuals (e.g., direct phone number and email); and
- General contact information (e.g., main phone number and support intake email).

Within ACME's cybersecurity function, TPRM analysts will contact the POC to deliver ACME's TPRM control questionnaire. Upon receiving the filled-out questionnaire, TPRM analysts:

- Validate the completion of the questionnaire and use available information to perform a TPRM assessment;
- Validate the statutory and/or regulatory requirements the TPSP must comply with as part of a contract with ACME; and
- Review the TPSP's online reputation to identify possible issues with the TPSP;
- As necessary:
    - Request additional information and/or interviews with the POC; and
    - Gather information regarding certifications, audit reports and other applicable items.

This phase involves determining and understanding the risks associated with TPSPs. This phase needs to be able to account for the following needs, since not all TPSP are equal:

- The level of rigor necessary;
- The most appropriate assessment method:
    - Manual Point In Time (MPIT);
    - Automated Point In Time (APIT); or
    - Automated Evidence with Human Review (AEHR); and
- The methodology that will be used to assess controls:
    - Qualitative;
    - Semi-Quantitative; or
    - Quantitative.

ACME recognizes four (4) options for managing risk:

(1) Reduce the risk to an acceptable level;
(2) Avoid the risk;
(3) Transfer the risk to another party; or
(4) Accept the risk.

See Appendix A: Risk Treatment Options for more information on ACME's approved risk treatment options.

TPRM Phase 2(A): Threat Identification

TPRM analysts review the TPSP's proposed product(s) and/or service(s) to identify possible threats to ACME. This includes screening TPSPs against sanction lists and other sources regarding ethical and/or compliance concerns to determine the inherent risk they pose to ACME.

See Appendix E: Threat Catalog for a list of reasonable natural and man-made threats. The use case for this threat catalog for TPRM purposes address the question, "***What natural and man-made threats affect control execution?***"

From a TPRM perspective, if the threat materializes, will the implemented TPRM controls function as expected? A threat can be defined according to use as either a noun or verb:

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

When an identified threat poses a material impact, that is a material threat. A material threat:

TPRM Phase 4: Due Care

Upon entering into a contract with a TPSP, the next phase in TPRM is for ACME to perform due care activities to ensure the TPSP maintains reasonable cybersecurity and data protection practices.

TPRM Phase 4(A): Ongoing Monitoring

Ongoing monitoring is essential for TPRM because it allows ACME to respond to evolving threats and risks. How ongoing monitoring is reported to ACME will depend on the contract in place with the TPSP. This may include automated feeds for continuous reporting or it may be a manual process that is up to ACME to initiate.

ACME should utilize Continuous Security Monitoring (CSM) tools to enable automated, real-time monitoring of its TPSPs. Depending on the capabilities of the CSM tool, it is possible to identify changes or vulnerabilities that occur with a TPSP that include, but are not limited to:

- Mergers, acquisitions & divestitures;
- Contract changes;
- Natural disasters;
- Legal or regulatory changes;
- Workforce changes;
- Negative media;
- Unethical business practices; and
- Financial stability.

TPRM Phase 4(B): Record Keeping and Reporting

Record-keeping and reporting involves utilizing a standardized process to efficiently and effectively maintain records associated with TPSPs. This can be done with specialized software or tools to assist in automating the process, but it can also be manual (e.g., desktop software such as Microsoft Excel or Word).

From a due care perspective, ACME should track and monitor the following TPSP-related information:

- Inventories;
- Risk assessments;
- Identified issues / incidents;
- Program compliance;
- Regulatory considerations; and
- New or emerging risks and threats.

The procurement team is responsible for compiling and reporting TPSP issues to relevant ACME stakeholders, including, but not limited to:

- TPRM analysts;
- Legal representatives;
- Risk committee; and
- Executive leadership.

TPRM reporting should be conducting on a consistent basis, following a regular reporting schedule applicable to ACME's procedures on no less than an annual basis.

APPENDICES

APPENDIX A: RISK TREATMENT OPTIONS

REDUCE RISK

When a risk is reduced, a plan is implemented to correct or remediate the issue to reduce risk to an acceptable level.

Risk reduction can be achieved through management controls or other arrangements which reduce the frequency of, or opportunity for, error, such as alternative procedures, quality assurance, testing, training, education, supervision, review, documented policy and procedures.

Examples of reducing risk include, but are not limited to:

- *Apply compensating controls.*
- *Remediate vulnerabilities to correct identified deficiencies.*

AVOID RISK

When a risk is avoided, a decision is made not to proceed with the activity.

Wherever possible, risk avoidance measures should be designed to be embedded in normal business processes, activities and systems. Those measures should not impede the logical or natural flow of existing processes and should be easy to understand and appreciate.

Examples of avoiding risk include, but are not limited to:

- *Terminate the project.*
- *Select a different solution that does not have the same risk.*

TRANSFER RISK

When risk is transferred, a plan is implemented that shares or transfers the risk away from ACME.

Risk can be transferred by shifting the responsibility for a risk to another party. Risks may be transferred in full, or they may be shared with another party. Risks should be allocated to the party that can exercise the most effective control over those risks.

Examples of transferring risk include, but are not limited to:

- *Purchase additional cybersecurity insurance.*
- *Select a TPSP that will accept indemnification for the risk associated with providing the service (e.g., PCI DSS payment processing).*

ACCEPT RISK

When risk is accepted, a decision is made to retain the risk and maintain the status quo without any remediation actions. While accepting risk is an option for management, the decision needs to be reasonably justified and documented.

Examples of reducing risk include, but are not limited to:

- *Continuing with the project, being fully aware of the risks.*
- *Choosing not to remediate vulnerabilities, based on untenable remediation costs.*

APPENDIX C: TPRM CYBERSECURITY & DATA PROTECTION CONTROLS

SCF CORE FUNDAMENTALS TPRM CONTROLS

ACME's TPRM controls are sourced from the Secure Controls Framework (SCF) and utilize the Cybersecurity Oversight, Resilience and Enablement (CORE) Fundamentals baseline.[16]

Control Count	SCF Control	SCF #	SCF CORE Fundamentals Control Description	Control Question
1	Publishing Cybersecurity & Data Protection Documentation	GOV-02	ACME expects its partners to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	Does the third-party establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures?
2	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	ACME expects its partners to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	Does the third-party assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program?
3	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	ACME expects its partners to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	Does the third-party compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control?
4	Asset Inventories	AST-02	ACME expects its partners to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	Does the third-party perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel?
5	Data Action Mapping	AST-02.8	ACME expects its partners to create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed.	Does the third-party create and maintain a map of technology assets where sensitive/regulated data is stored, transmitted or processed?

[16] *SCF CORE Fundamentals - https://securecontrolsframework.com/core/*

APPENDIX D: MATURITY MODEL

The SCF C|P-CMM draws upon the high-level structure of the Systems Security Engineering Capability Maturity Model v2.0 (SSE-CMM), since we felt it was the best model to demonstrate varying levels of maturity for people, processes and technology at a control level. If you are unfamiliar with the SSE-CMM, it is well-worth your time to read through the SSE-CMM Overview Document that is hosted by the US Defense Technical Information Center (DTIC).[17]

The six (6) C|P-CMM levels are:

(1) CMM 0 – Not Performed
(2) CMM 1 – Performed Informally
(3) CMM 2 – Planned & Tracked
(4) CMM 3 – Well-Defined
(5) CMM 4 – Quantitatively Controlled
(6) CMM 5 – Continuously Improving

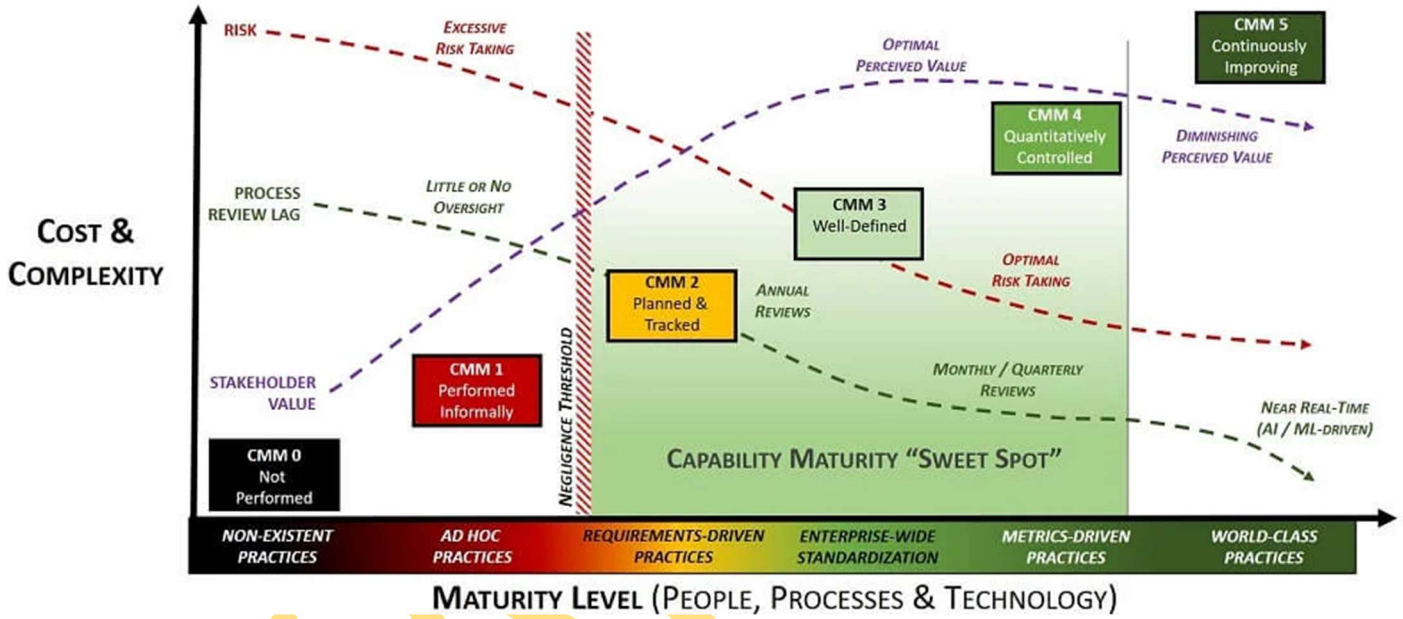

Figure D-1. SCF Maturity Model

C|P-CMM LEVEL 0 (L0) – NOT PERFORMED

This level of maturity is defined as "non-existence practices," where the control is not being performed:

- Practices are non-existent, where a reasonable person would conclude the control is not being performed.
- Evidence of due care and due diligence do not exist to demonstrate compliance with applicable statutory, regulatory and/or contractual obligations.

L0 practices, or a lack thereof, are generally considered to be negligent. The reason for this is if a control is reasonably-expected to exist, by not performing the control that is negligent behavior. The need for the control could be due to a law, regulation or contractual obligation (e.g., client contract or industry association requirement).

Note – The reality with a L0 level of maturity is often:

- For smaller organizations, the IT support role only focuses on "break / fix" work or the outsourced IT provider has a scope in its support contract that excludes the control through either oversight or ignorance of the client's requirements.
- For medium / large organizations, there is IT and/or cybersecurity staff, but governance is functionally non-existent and the control is not performed through either oversight, ignorance or incompetence.

[17] *SCF C|P-CMM - https://securecontrolsframework.com/free/capability-maturity-model/*

C|P-CMM Level 1 (L1) – Performed Informally

This level of maturity is defined as "ad hoc practices," where the control is being performed, but lacks completeness & consistency:

- Practices are "ad hoc" where the intent of a control is not met due to a lack consistency and formality.
- When the control is met, it lacks consistency and formality (e.g., rudimentary practices are performed informally).
- A reasonable person would conclude the control is not consistently performed in a structured manner.
- Performance depends on specific knowledge and effort of the individual performing the task(s), where the performance of these practices is not proactively governed.
- Limited evidence of due care and due diligence exists, where it would be difficult to legitimately disprove a claim of negligence for how cybersecurity/privacy controls are implemented and maintained.
- L1 practices are generally considered to be negligent. The reason for this is if a control is reasonably-expected to exist, by only implementing ad-hoc practices in performing the control that could be considered negligent behavior. The need for the control could be due to a law, regulation or contractual obligation (e.g., client contract or industry association requirement).

Note – The reality with a L1 level of maturity is often:

- For smaller organizations, the IT support role only focuses on "break / fix" work or the outsourced IT provider has a limited scope in its support contract.
- For medium / large organizations, there is IT and/or cybersecurity staff but there is no management focus to spend time or resources on the control.

C|P-CMM Level 2 (L2) – Planned & Tracked

Practices are "requirements-driven" where the intent of control is met in some circumstances, but not standardized across the entire organization:

- Practices are "requirements-driven" (e.g., specified by a law, regulation or contractual obligation) and are tailored to meet those specific compliance obligations (e.g., evidence of due diligence).
- Performance of a control is planned and tracked according to specified procedures and work products conform to specified standards (e.g., evidence of due care).
- Controls are implemented in some, but not all applicable circumstances/environments (e.g., specific enclaves, facilities or locations).
- A reasonable person would conclude controls are "compliance-focused" to meet a specific obligation, since the practices are applied at a local/regional level and are not standardized practices across the enterprise.
- Sufficient evidence of due care and due diligence exists to demonstrate compliance with specific statutory, regulatory and/or contractual obligations.
- L2 practices are generally considered to be "audit ready" with an acceptable level of evidence to demonstrate due diligence and due care in the execution of the control. L2 practices are generally targeted on specific systems, networks, applications or processes that require the control to be performed for a compliance need (e.g., PCI DSS, HIPAA, CMMC, NIST 800-171, etc.).

It can be argued that L2 practices focus more on compliance over security. The reason for this is the scoping of L2 practices are narrowly-focused and are not enterprise-wide.

Note – The reality with a L2 level of maturity is often:

- For smaller organizations:
  - IT staff have clear requirements to meet applicable compliance obligations or the outsourced IT provider is properly scoped in its support contract to address applicable compliance obligations.
  - It is unlikely that there is a dedicated cybersecurity role and at best it is an additional duty for existing personnel.
- For medium / large organizations:
  - IT staff have clear requirements to meet applicable compliance obligations.
  - There is most likely a dedicated cybersecurity role or a small cybersecurity team.

C|P-CMM Level 3 (L3) – Well-Defined

This level of maturity is defined as "enterprise-wide standardization," where the practices are well-defined and standardized across the organization:

- Practices are standardized "enterprise-wide" where the control is well-defined and standardized across the entire enterprise.

APPENDIX E: THREAT CATALOG

The use case for this threat catalog for Third-Party Risk Management (TPRM) purposes address the question, "***What natural and man-made threats affect control execution?***" From a TPRM perspective, if the threat materializes, will the implemented TPRM controls function as expected?

A threat can be defined according to use as either a noun or verb:

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

NATURAL THREATS

Natural threats consist of the following fourteen (14) categories from the Secure Controls Framework (SCF) threat catalog:[18]

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, it envisions 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.

[18] *SCF Threat Catalog - https://securecontrolsframework.com/*