Cybersecurity & Data Privacy Risk Management Model (C|P-RMM) Overview

Version 2025.1

Table of Contents

EXECUTIVE SUMMARY

To help simplify risk management practices, ComplianceForge and the Secure Controls Framework (SCF) jointly developed the Cybersecurity & Data Privacy Risk Management Model (C|P-RMM). The concept of creating the C|P-RMM was to establish an efficient methodology to identify, assess, report and mitigate risk across the entire organization.

The C|P-RMM:

- Is a free solution that organizations can use to holistically approach that breaks risk management down into seventeen (17) distinctive steps;
- Exists is to help cybersecurity and data privacy functions create a repeatable methodology to identify, assess, report and mitigate risk;
- Offers flexibility to report on risk at a control level or aggregate level (e.g., a project, department, domain or organization-level); and
- Guides the decision to a risk treatment option (e.g., reduce, avoid, transfer or accept).

The most important concept to understand in cybersecurity and data privacy-related risk management is that the cybersecurity and IT departments generally do not "own" technology-related risks, since that "risk ownership" primarily resides with Line of Business (LOB) management. An organization's cybersecurity and data privacy functions serve as the primary mechanism to educate those LOB stakeholders on identified risks and provide possible risk treatment solutions. Right or wrong, LOB management is ultimately responsible to decide how risk is to be handled.

Where the C|P-RMM exists to help cybersecurity and data privacy functions create a repeatable methodology to identify, assess, report and mitigate risk. This is based on the understanding that the responsibility to approve a risk treatment solution rests with the management of the LOB/department/team/stakeholder that "owns" the risk. The C|P-RMM is meant to guide the decision to one of these common risk treatment options:

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

It is a common problem for individuals who are directly impacted by risk to simply claim, *"I accept the risk"* in a misplaced maneuver to make the risk go away, so that the project/initiative can proceed without having to first address deficiencies. This is why it is critically important that as part of a risk management program to identify the various levels of management who have the legitimate authority to make risk management decisions. This can help prevent low-level managers from recklessly accepting risk that should be reserved for more senior management.

Fundamentally, risk management requires educating stakeholders for situational awareness and decision-making purposes, where reporting risk can be summarized by explaining the "health" of the cybersecurity and data privacy program as to how the assessed controls provide assurance that the organization's stated risk tolerance is or is not achieved. Therefore, the goal of the C|P-RMM is to categorize the risk assessment results according to one (1) of the following four (4) risk determinations:

1. Strictly Conforms;
2. Conforms;
3. Significant Deficiency; or
4. Material Weakness

The intent of having these risk determinations is to normalize the terminology associated with the level of conformity an organization conforms to its applicable cybersecurity and data protection controls. This methodology can help an organization adhere to its risk appetite.

INTRODUCTION

The C|P-RMM is designed to be an integral tool of an organization's ability to demonstrate evidence of due diligence and due care. This not only benefits your organization by having solid risk management practices, but it can also serve as a way to reduce risk for those who have to initiate the hard discussions on risk management topics.

"DON'T SHOOT THE MESSENGER" PROTECTIONS

If you worry about having to preface risk management discussions with, *"Don't shoot the messenger!"* then the C|P-RMM can be an additional layer of protection for your professional reputation. Where the C|P-RMM benefits security, technology and privacy personnel is the potential "get out of jail" documentation that quality risk assessments and risk management practices can provide. Just like with compliance documentation, if risk management discussions are not documented then risk management practices do not exist.

Before you read further, ask yourself these two (2) questions about your organization and your personal exposure in risk management:

1. Can you prove that the right people within your organization are both aware of risks and have taken direct responsibility for mitigating those risks?
2. If there was a breach or incident that is due to identified risks that went unmitigated, where does the "finger pointing" for blame immediately go to?

Instead of executive leadership hanging blame on the CIO or CISO, quality risk management documentation can prove that reasonable steps were taken to identify, assess, report and mitigate risk. This type of documentation can provide evidence of due diligence and due care on the part of the CIO/CISO/CRO, which firmly puts the responsibility back on the management of the team/department/line of business that "owns" the risk.

Organizations often face conflicting expectations for risk management, based on department-level practices. For example, where disjointed risk management practices exist, a "Moderate Risk" often has entirely different financial and/or operational impacts across cybersecurity, IT, legal, finance, HR, operations, etc. The concept of Enterprise Risk Management (ERM) is to apply a comprehensive, organization-wide approach to risk management practices, where each department operates according to a similar playbook, where "Moderate Risk" means the same thing across the entire organization. This helps make an "apples to apples" comparison that can aid in creating a more holistic approach to risk management practices when risk designations are standardized.

Risk management activities are logical and systematic processes that can be used when making well-informed decisions to improve effectiveness and efficiency. Proactive risk management activities have these characteristics:

- Integrated into Business As Usual (BAU) activities (e.g., everyday work);
- Focuses on proactive management involvement, rather than reactive crisis management;
- Identifies and helps prepare for what might happen;
- Identifies opportunities to improve performance; and
- Proposes taking action to:
  - Avoid or reduce unwanted exposures; and/or
  - Maximize opportunities identified.

The articulation of risk management concepts is both an art and science. This requires a clear understanding of certain risk management terminology:

- Risk Appetite;
- Risk Tolerance; and
- Risk Threshold.

Risk management decisions must be explained in the context of the business, since risk management practices do not operate in a vacuum. Therefore, it is crucial to understand the environment where risk management practices exist. This also requires a clear understanding of business planning terminology:

- Mission;
- Vision; and
- Strategy.

From a hierarchical perspective:

- An organization's risk appetite exists at the corporate level to influence actions and decisions, specifically the organization's strategy. The strategy provides prioritization and resourcing constraints to the organization's various Line of Business (LOB).
- The risk appetite helps define the organization's risk tolerance to influence actions and decisions at the LOB level. Risk tolerance influences objectives, maturity targets and resource prioritization.
- Risk thresholds affect actions and decisions at the department and team levels. Risk thresholds influence processes, technologies, staffing levels and the supply chain (e.g., vendors, suppliers, consultants, contractors, etc.). Defined risk thresholds provide criteria to assess operational risks that exist in the course of conducting business.

It is acceptable for risk management practices to be:

- Quantifiable (objective);
- Qualifiable (subjective); or
- A hybrid approach that clearly identifies the subjective and object nature of risk analysis practices.

What is important to keep at the forefront of risk management considerations is the material nature of risk, as it pertains to the organization. Risks that have a material impact include, but are not limited to:

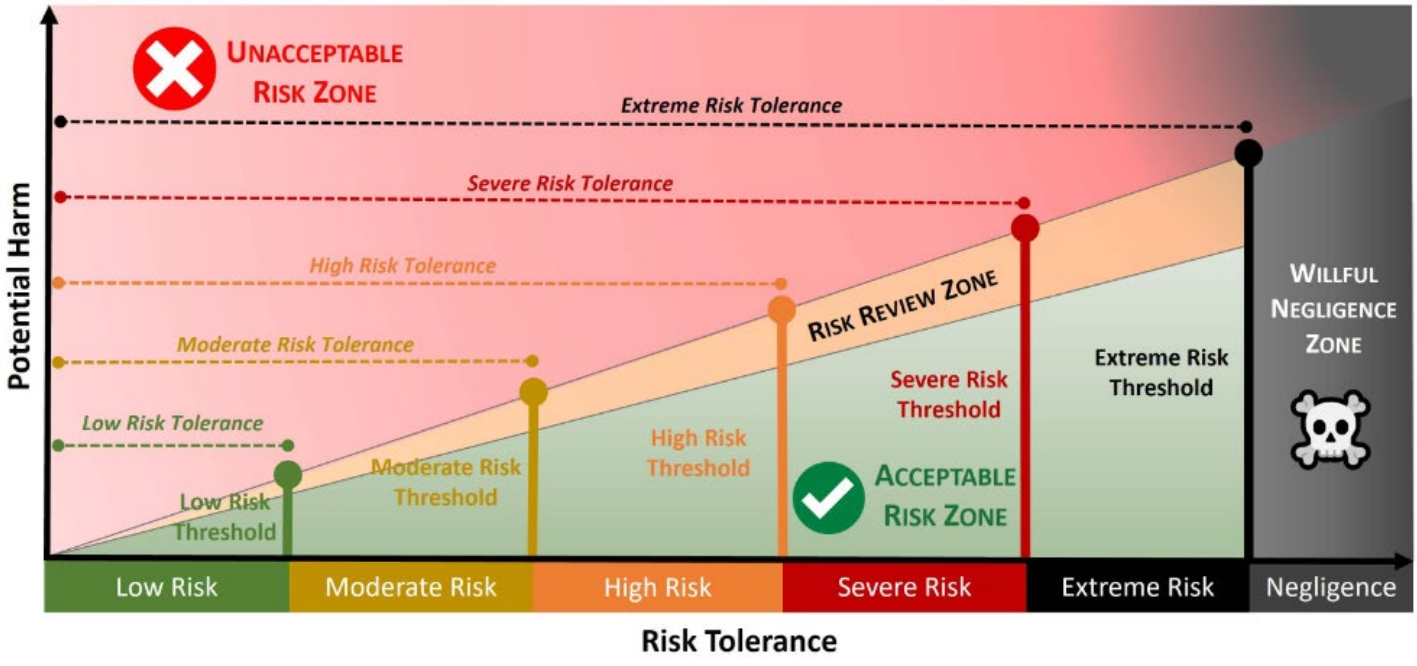
- Confidentiality, Integrity, Availability & Safety (CIAS) of the organization's sensitive/regulated data;
- Supply chain security;
- Macroeconomic forces;
- Socio-political changes;
- Statutory / regulatory changes;
- Competitive landscape;
- Diplomatic sanctions (e.g., taxes, customs, embargoes, etc.); and
- Natural / manmade disasters (e.g., pandemics, war, etc.).

BASELINING RISK MANAGEMENT TERMINOLOGY

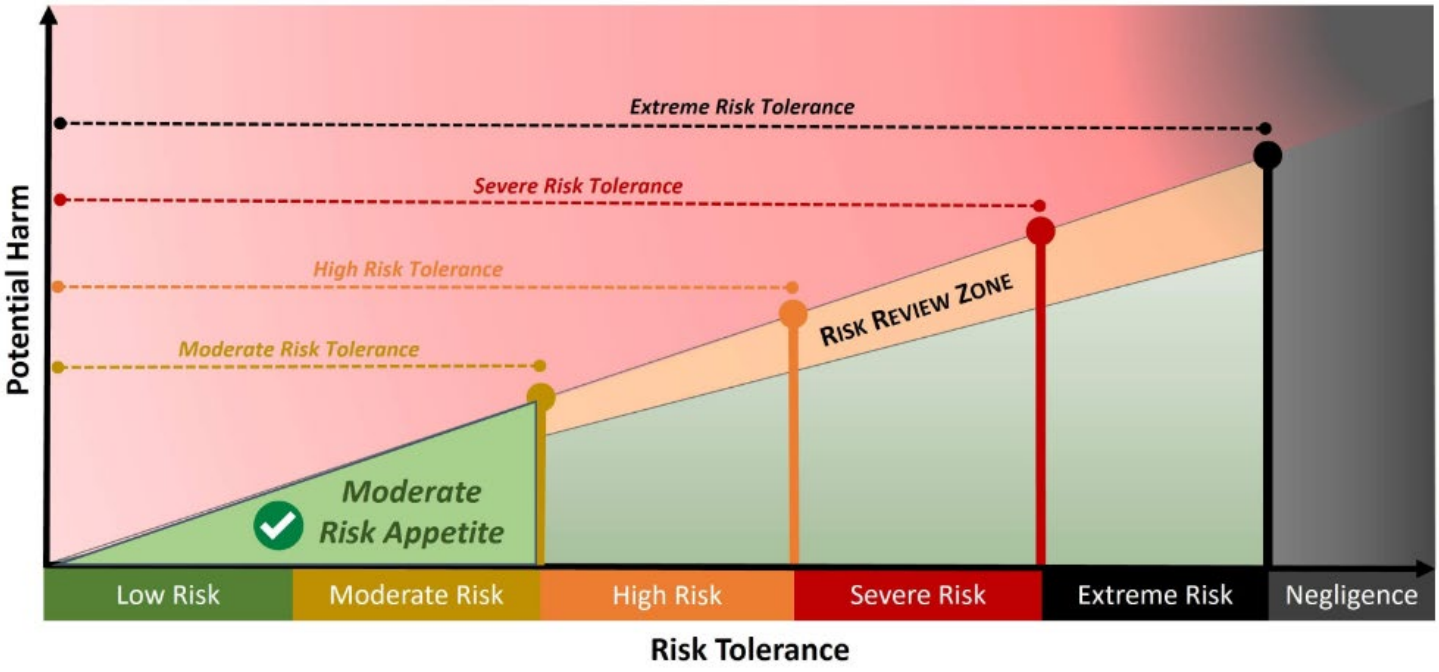
Risk management involves coordinated activities that optimize the management of potential opportunities and adverse effects. Proactive risk management activities provide a way to realize potential opportunities without exposing an organization to unnecessary peril.

The goal of risk analysis is to determine the potential negative implications of an action or situation to determine one (1) of two (2) decisions:

1. **Acceptable Risk**: the criteria fall within a range of acceptable parameters; or
2. **Unacceptable Risk**: The criteria fall outside a range of acceptable parameters.



Building upon the graphic listed above, when viewed from a risk appetite perspective, for an organization that wants to follow a Moderate Risk Appetite, which establishes constraints for allowable and prohibited activities, based on the potential harm to the organization:

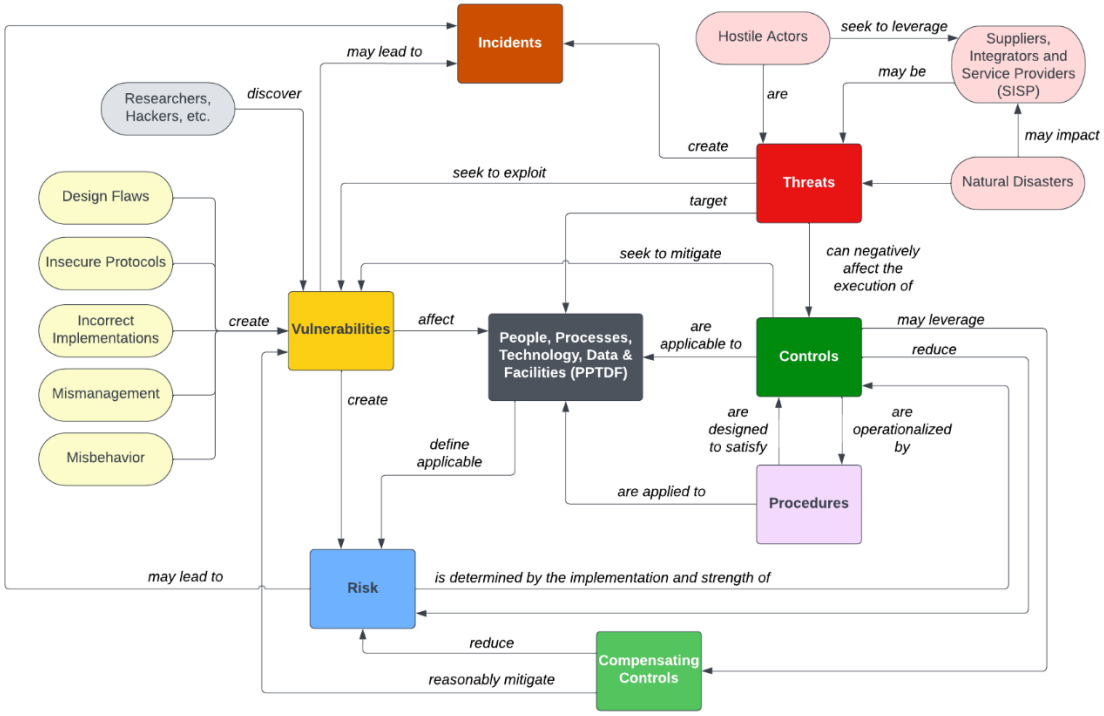


Understanding The Differences Between: Risks vs Threats

Risks and threats both tie into cybersecurity and data privacy controls, but it is important to understand the differences:

- A risk exists due to the absence of or a deficiency with a control; but
- A threat affects the ability of a control to exist or operate properly.

ComplianceForge published a "threats vs vulnerabilities vs risks" informational graphic that describes the relationship between these components. That informational graphic is shown below:[1]



[1] *Risk vs Threat vs Vulnerability Ecosystem - https://complianceforge.com/content/pdf/guide-risk-vs-threat-vs-vulnerability-ecosystem.pdf*

What Is A Risk?

In the context of cybersecurity & data privacy practices, "risk" is defined as:

- 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.*

In the context of this definition of risk, it is important to define underlying components of this risk definition:

- Danger: *state of possibly suffering harm or injury.*
- Harm: *material / physical damage.*
- Loss: *destruction, deprivation or inability to use.*

What Is A Threat?

In the context of cybersecurity & data privacy practices, "threat" is defined as:

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

Understanding The Differences Between: Risk Tolerance vs Risk Threshold vs Risk Appetite

Key concepts associated with risk management include:

- Risk Appetite: The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value.[2]
- Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a desired result.[3]
- Risk Threshold: Values used to establish concrete decision points and operational control limits to trigger management action and response escalation.[4]

What Is A Risk Appetite?

A risk appetite is a broad "risk management concept" that is used to inform employees about what is and is not acceptable, in terms of risk management from an organization's executive leadership team.

A risk appetite does not contain granular risk management criteria and is primarily a "management statement" that is subjective in nature. Similar in concept to how a policy is a *"high-level statement of management intent,"* an organization's defined risk appetite is a high-level statement of how all, or certain types of, risk are willing to be accepted.[5]

Examples of an organization stating its risk appetite from basic to more complex statements:

- *"[organization name] is a low-risk organization and will avoid any activities that could harm its customers."*
- *"[organization name] will aggressively pursue innovative solutions through Research & Development (R&D) to provide industry-leading products and services to our clients, while maintaining a Moderate Risk Appetite. Developing breakthrough products and services does invite potential risk through changes to traditional supply chains, disruptions to business operations and changing client demand. Proposed business practices that pose greater than a Moderate Risk will be considered on a case-by-case basis for financial, operational and legal implications."*

It is important to point out that in many immature risk programs, risk appetite statements are divorced from reality. Executive leaders mean well when they issue risk appetite statements, but the Business As Usual (BAU) practices routinely violate the risk appetite. This is often due to numerous reasons that include, but are not limited to:

- Technical debt;
- Dysfunctional management decisions;
- Insecure practices;
- Inadequate funding/resourcing;
- Improperly scoped support contracts (e.g., Managed Service Providers (MSPs), consultants, vendors, etc.); and
- Lack of pre-production security testing.

---

[2] *NIST Glossary for Risk Appetite - https://csrc.nist.gov/glossary/term/risk_appetite*
[3] *NIST Glossary for Risk Tolerance - https://csrc.nist.gov/glossary/term/risk_tolerance*
[4] *NIST Glossary for Thresholds - https://csrc.nist.gov/glossary/term/thresholds*
[5] *ComplianceForge Hierarchical Cybersecurity Governance Framework (HCGF) - https://complianceforge.com/content/pdf/complianceforge-hierarchical-cybersecurity-governance-framework.pdf*

What Is A Risk Tolerance?

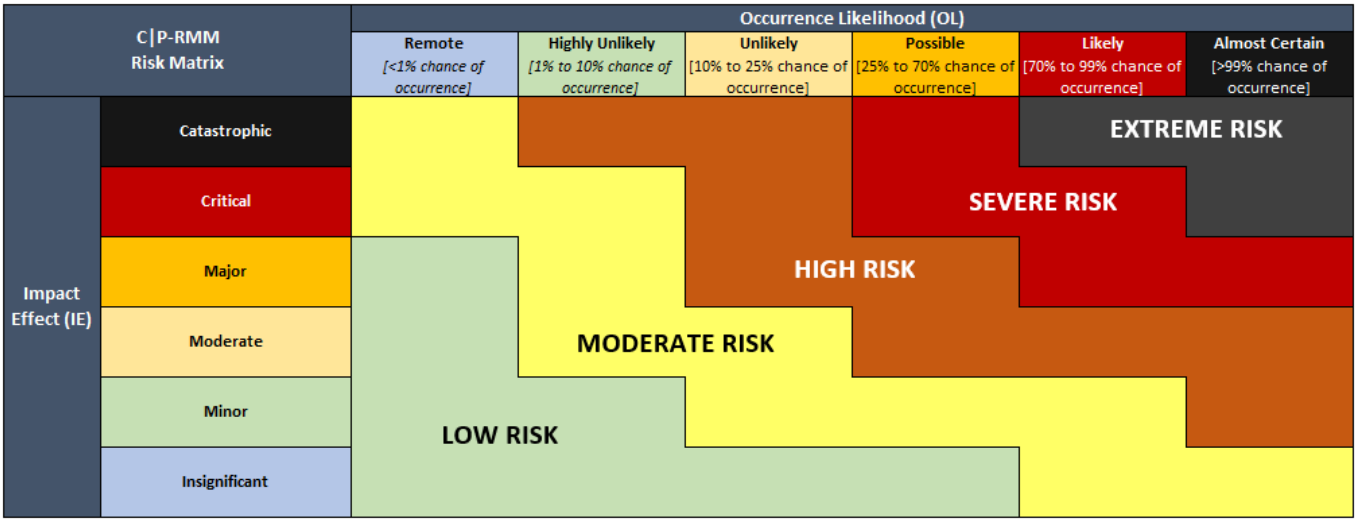
Risk tolerance is based on objective criteria, unlike the subjective, conceptual nature of a risk appetite. Defining objective criteria is a necessary step to be able to categorize risk on a graduated scale. Establishing objective criteria to quantify the impact of a risk enables risk assessments to leverage that same criteria and assist decision-makers in their risk management decisions (e.g., accept, mitigate, transfer or avoid).

From a graduated scale perspective, it is possible to define "tolerable" risk criteria to create five (5) useful categories of risk:

1. Low Risk;
2. Moderate Risk;
3. High Risk;
4. Severe Risk; and
5. Extreme Risk.

There are two (2) objective criteria that go into defining what constitutes a low, moderate, high, severe or Extreme Risk includes:

1. Impact Effect (IE); and
2. Occurrence Likelihood (OL).



The six (6) categories of IE are:

1. Insignificant *(e.g., organization-defined little-to-no impact to business operations);*
2. Minor *(e.g., organization-defined minor impacts to business operations)*;
3. Moderate *(e.g., organization-defined moderate impacts to business operations)*;
4. Major *(e.g., organization-defined major impacts to business operations)*;
5. Critical *(e.g., organization-defined critical impacts to business operations)*; and
6. Catastrophic *(e.g., organization-defined catastrophic impacts to business operations).*

The six (6) categories of OL are:

1. Remote possibility *(e.g., <1% chance of occurrence)*;
2. Highly unlikely *(e.g., from 1% to 10% chance of occurrence)*;
3. Unlikely *(e.g., from 10% to 25% chance of occurrence)*;
4. Possible *(e.g., from 25% to 70% chance of occurrence)*;
5. Likely *(e.g., from 70% to 99% chance of occurrence)*; and
6. Almost certain *(e.g., >99% chance of occurrence)*.

There are three (3) general approaches are commonly employed to estimate OL:

1. Relevant historical data;
2. Probability forecasts; and
3. Expert opinion.

An organization's risk tolerance is influenced by several factors that includes, but is not limited to:

- Statutory, regulatory and contractual compliance obligations (including adherence to privacy principles for ethical data protection practices).
- Organization-specific threats (natural and manmade).
- Reasonably expected industry practices.
- Pressure from competition.
- Executive management decisions.

LOW RISK TOLERANCE

Organizations that would be reasonably expected to adopt a Low Risk Tolerance generally:

- Provide products and/or services that are necessary for the population to maintain normalcy in daily life.
- Are in highly regulated industries with explicit cybersecurity and/or data privacy requirements.
- Store, process and/or transmit highly sensitive/regulated data.
- Are legitimate targets for nation-state actors to disrupt and/or compromise due to the high-value nature of the organization.
- Have strong executive management support for cybersecurity and data privacy practices as part of "business as usual" activities.
- Maintain a high level of capability maturity for preventative cybersecurity controls to implement "defense in depth" protections across the enterprise.
- Have a high level of situational awareness (cybersecurity & physical) that includes its supply chain.
- Have cyber-related liability insurance.

Organizations that are reasonably expected to operate with a Low Risk Tolerance include, but are not limited to:

- Critical infrastructure
- Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.)
- Telecommunications (e.g., Internet Service Providers (ISPs), mobile phone carriers, Cloud Service Providers (CSPs), etc.) (high value)
- Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.)
- Technology Research & Development (R&D) (high value)
- Healthcare (high value)
- Government institutions:
    - Military
    - Law enforcement
    - Judicial system
    - Financial services (high value)
    - Defense Industrial Base (DIB) contractors (high value)

MODERATE RISK TOLERANCE

Organizations that would be reasonably expected to adopt a Moderate Risk Tolerance generally:

- Have executive management support for securing sensitive / regulated data enclaves.
- Are in regulated industries that have specific cybersecurity and/or data privacy requirements (e.g., CMMC, PCI DSS, SOX, GLBA, RMF, etc.).
- Have "flow down" requirements from customers that require adherence to certain cybersecurity and/or data privacy requirements.
- Store, process and/or transmit sensitive/regulated data.
- Are legitimate targets for attackers who wish to financially benefit from stolen information or ransom.
- Have cyber-related liability insurance.

Organizations that are reasonably expected to operate with a Moderate Risk Tolerance include, but are not limited to:

- Education (e.g., K-12, colleges, universities, etc.)
- Utilities (e.g., electricity, drinking water, natural gas, sanitation, etc.)
- Telecommunications (e.g., Internet Service Providers (ISPs), mobile phone carriers, etc.)
- Transportation (e.g., airports, railways, ports, tunnels, fuel delivery, etc.)
- Technology services (e.g., Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), etc.)
- Manufacturing (high value)
- Healthcare
- Defense Industrial Base (DIB) contractors and subcontractors

- Legal services (e.g., law firms)
- Construction (high value)

HIGH RISK TOLERANCE

Organizations that would be reasonably expected to adopt a High Risk Tolerance generally:

- Are in an unregulated industry, pertaining to cybersecurity and/or data privacy requirements.
- Do not store, process and/or transmit sensitive/regulated data.
- Lack management support for cybersecurity and data privacy governance practices.
- Do not have cyber-related liability insurance.

Organizations that may choose to operate with a High Risk Tolerance include, but are not limited to:

- Startups
- Hospitality industry (e.g., restaurants, hotels, etc.)
- Construction
- Manufacturing
- Personal services

SEVERE RISK TOLERANCE

Organizations that would be reasonably expected to adopt a Severe Risk Tolerance generally:

- Are in an unregulated industry, pertaining to cybersecurity and/or data privacy requirements.
- Do not store, process and/or transmit sensitive/regulated data.
- Lack management support for cybersecurity and data privacy governance practices.
- Do not have cyber-related liability insurance.

Organizations that may choose to operate with a High Risk Tolerance include, but are not limited to:

- Startups
- Artificial Intelligence (AI) developers

EXTREME RISK TOLERANCE

Organizations that would be reasonably expected to adopt an Extreme Risk Tolerance generally:

- Are in an unregulated industry, pertaining to cybersecurity and/or data privacy requirements.
- Do not store, process and/or transmit sensitive/regulated data.
- Lack management support for cybersecurity and data privacy governance practices.
- Do not have cyber-related liability insurance.

Organizations that may choose to operate with a High Risk Tolerance include, but are not limited to:

- Startups
- Artificial Intelligence (AI) developers

WHAT IS A RISK THRESHOLD?

Risk thresholds are directly tied to risk tolerance and utilize organization-specific criteria (e.g., acceptable and unacceptable parameters). These risk thresholds exist between the different levels of risk tolerance (e.g., between Low Risk and Moderate Risk, between Moderate Risk and High Risk, etc.). By establishing these risk thresholds, it brings the "graduated scale perspective" to life for risk management practices. Risk thresholds are criteria that are unique to an organization:

- Organization-specific activities / scenarios that could damage the organization's reputation;
- Organization specific activities / scenarios that could negatively affect short-term and long-term profitability; and
- Organization specific activities / scenarios that could impede business operations.

Risk thresholds are entirely unique to each organization, based on several factors that include:

- Financial stability;
- Management preferences;
- Compliance obligations (e.g., statutory, regulatory and/or contractual); and
- Insurance coverage limits.

What Is Materiality?

The SCF defines materiality as, *"A deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data privacy controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance."*[6]

The intended usage of materiality is meant to provide relevant context, as it pertains to risk thresholds. This is preferable when compared to relatively hollow risk findings that act more as guidelines than actionable, decision-making criteria. Cybersecurity materiality is meant to act as a "guard rail" for risk management decisions. A material weakness crosses an organization's risk threshold by making an actual difference to the organization, where systems, applications, services, personnel, the organization and/or third-parties are, or may be, exposed to an unacceptable level of risk.

The SEC, Generally Accepted Accounting Principles (GAAP) and International Financial Reporting Standards (IFRS) lack specificity in defining the criteria for materiality. Therefore, organizations generally have leeway to define it on their own. The lack of authoritative definition for materiality is not unique, since the concept of risk appetite, risk tolerance and risk threshold also suffer from nebulous definitions by statutory and regulatory authorities. For an item to be considered material, the control deficiency, risk, threat or incident (singular or a combination) generally must meet one or more of the following criteria where the potential financial impact is:[7]

- ≥ 5% of pre-tax income
- ≥ 0.5% of total assets
- ≥ 1% of total equity (shareholder value); and/or
- ≥ 0.5% of total revenue.

With evolving regulatory requirements for public disclosures, it is increasingly important to understand the nuances between material weakness vs material risk vs material threat vs material incident, since they have specific meanings:

Material Weakness

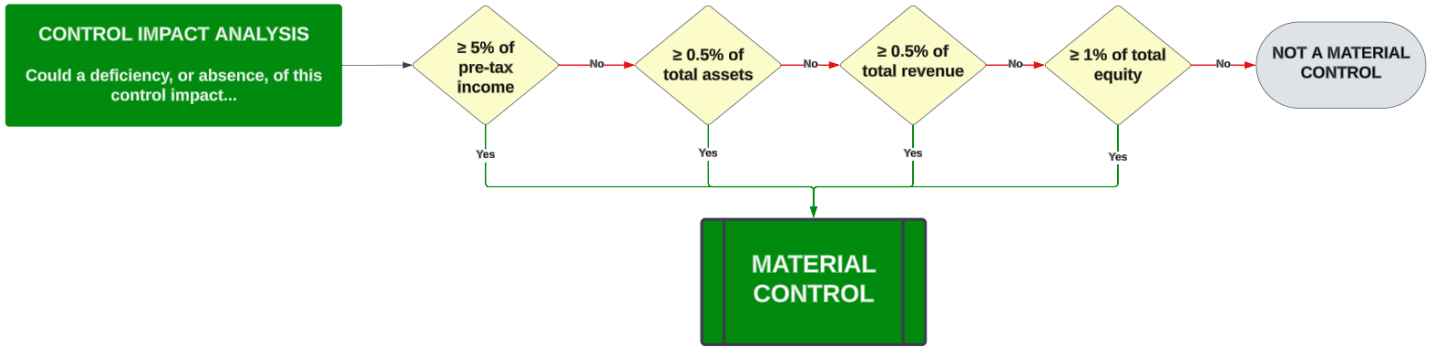
A material weakness is a deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data privacy controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance.

- When there is an existing deficiency (e.g., control deficiency) that poses a material impact, that is a material weakness (e.g., inability to maintain access control, lack of situational awareness to enable the timely identification and response to incidents, lacking pre-production control validation testing, etc.).
- A material weakness will be identified as part of a gap assessment, audit or assessment as a finding due to one or more control deficiencies.
- A material weakness should be documented in an organization's Plan of Action & Milestones (POA&M), risk register, or similar tracking mechanism used for remediation purposes.

Material Control

When a deficiency, or absence, of a specific control poses a material impact, that control is designated as a material control. A material control is such a fundamental cybersecurity and/or data protection control that:

- It is not capable of having compensating controls; and
- Its absence, or failure, exposes an organization to such a degree that it could have a material impact.

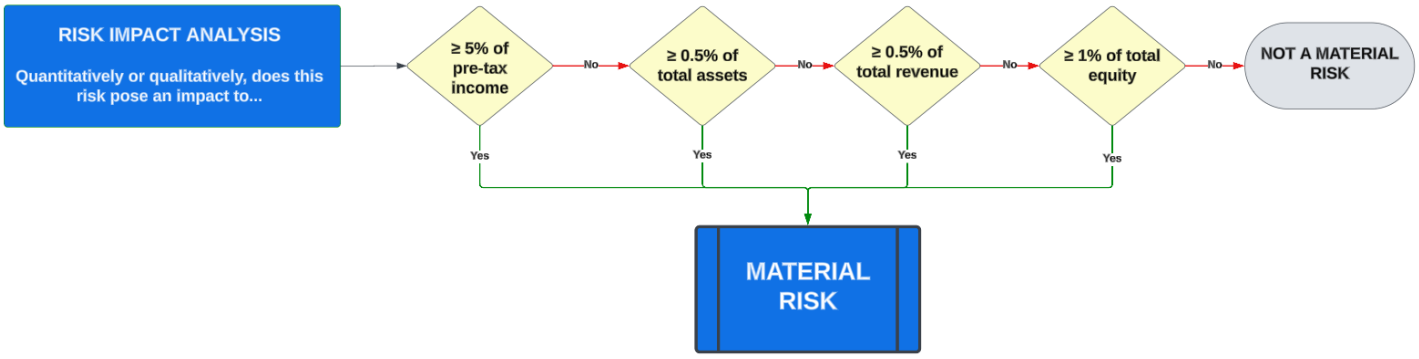


[6] *SCF Cybersecurity Materiality - https://securecontrolsframework.com/cybersecurity-materiality/*
[7] *Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf*

Material Risk

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

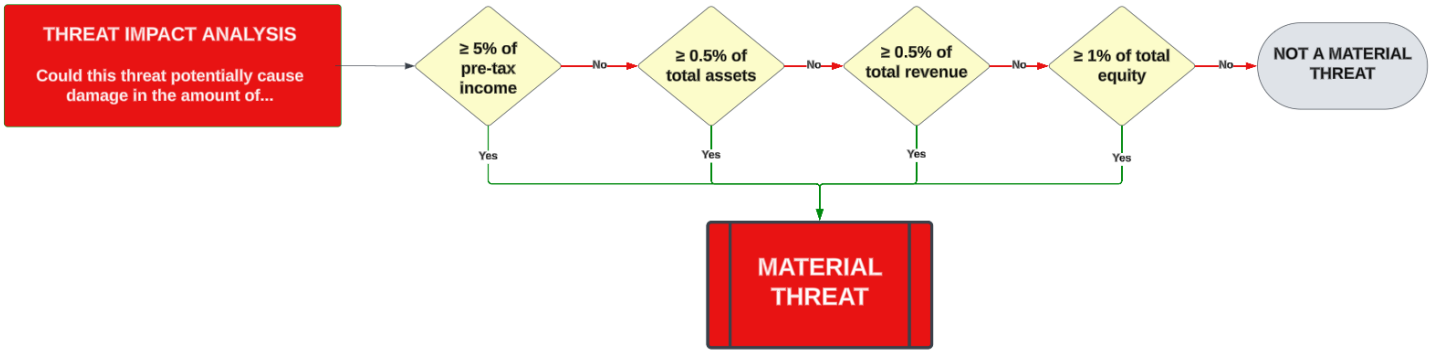
- Is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.); and
- Should be identified and documented in an organization's "risk catalog" that chronicles the organization's relevant and plausible risks.



Material Threat

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

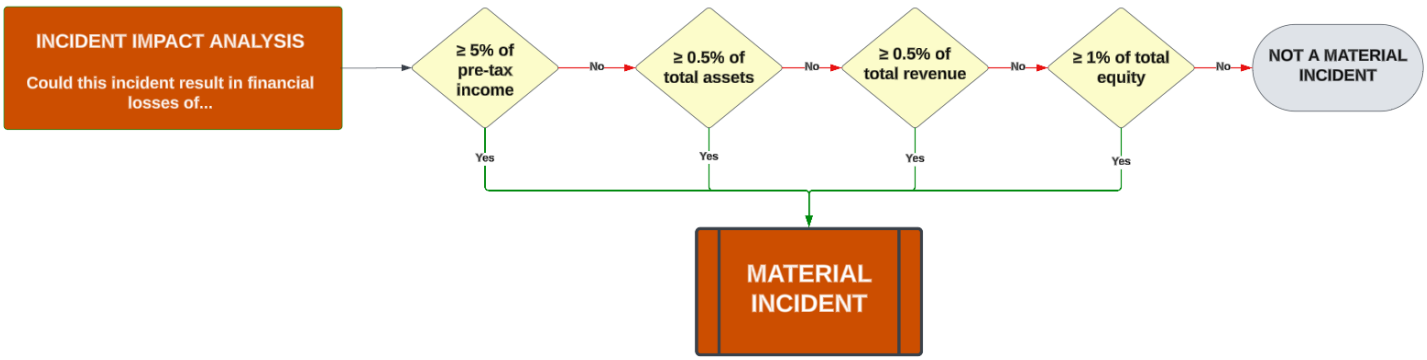
- Is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and
- Should be identified and documented in an organization's "threat catalog" that chronicles the organization's relevant and plausible threats.



Material Incident

When an incident poses a material impact, that is a material incident. A material incident is an occurrence that does or has the potential to:

- Jeopardize the Confidentiality, Integrity, Availability and/or Safety (CIAS) of a system, application, service or the data that it processes, stores and/or transmits with a material impact on the organization; and/or
- Constitute a violation, or imminent threat of violation, of an organization's policies, standards, procedures or acceptable use practices that has a material impact (e.g., malware on sensitive and/or regulated systems, emergent AI actions, illegal conduct, business interruption, etc.).



Historical Context For Cybersecurity & Data Privacy Materiality Usage

For Governance, Risk Management & Compliance (GRC) practitioners, materiality is often relegated to Sarbanes-Oxley Act (SOX) compliance. However, the concept of materiality is much broader than SOX and can be applied as part of risk reporting in any type of conformity assessment. Financial-related materiality definitions focus on investor awareness of third-party practices, not inwardly looking for adherence to an organization's risk tolerance:

- Per the Security and Exchange Commission (SEC), information is material *"to which there is a substantial likelihood that a reasonable investor would attach importance in determining whether to purchase the security registered."*[8]
- Per the International Accounting Standards Board (IASB), information is material, *"if omitting, misstating or obscuring it could reasonably be expected to influence the decisions that the primary users of general purpose financial statements make on the basis of those financial statements, which provide financial information about a specific reporting entity."*[9]

In legal terms, "material" is defined as something that is relevant and significant:

- In a lawsuit, "material evidence" is distinguished from totally irrelevant or of such minor importance that the court will either ignore it, rule it immaterial if objected to, or not allow lengthy testimony upon such a matter.
- A "material breach" of a contract is a valid excuse by the other party not to perform. However, an insignificant divergence from the terms of the contract is not a material breach.

Risk Management Options

Traditional risk management practices have four (4) options to address identified 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.

In a mature risk program, the results of risk assessments are evaluated with the organization's risk appetite in consideration. For example, if the organization has a Moderate Risk Appetite and there are several findings in a risk assessment that are High Risk, then action must be taken to reduce the risk. Accepting a High Risk would violate the Moderate Risk Appetite set by management. In reality, which leaves remediation, transferring or avoiding as the remaining three (3) options, since accepting the risk would be prohibited.

Practical Risk Management Example

For an example scenario, a theoretical company is experimenting with Artificial Intelligence (AI) to strengthen its products and/or services. Its long-standing risk appetite is relatively conservative, where the company draws a hard line that any risk over Moderate is unacceptable. Additionally, the company has zero tolerance for any activities that could harm its customers (e.g., physically or financially).

Given the necessary changes to ramp up both talent and technology to put the appropriate solutions in place to meet the company's deadlines, there are gaps/deficiencies. When the risk management team assesses the associated risks, the results identify a range of risks from High to Extreme. The reason for these results is simply due to the higher likelihood of emergent behaviors occurring from AI that potentially could harm individuals (e.g., catastrophic impact effect). The results were objective and told a compelling story that there is a realistic chance of significant damage to the company's reputation and financial liabilities from class action lawsuits.

With those results that point to risks exceeding the organization's risk appetite, it is a management decision on how to proceed. What does the CEO / Board of Directors (BoD) do?

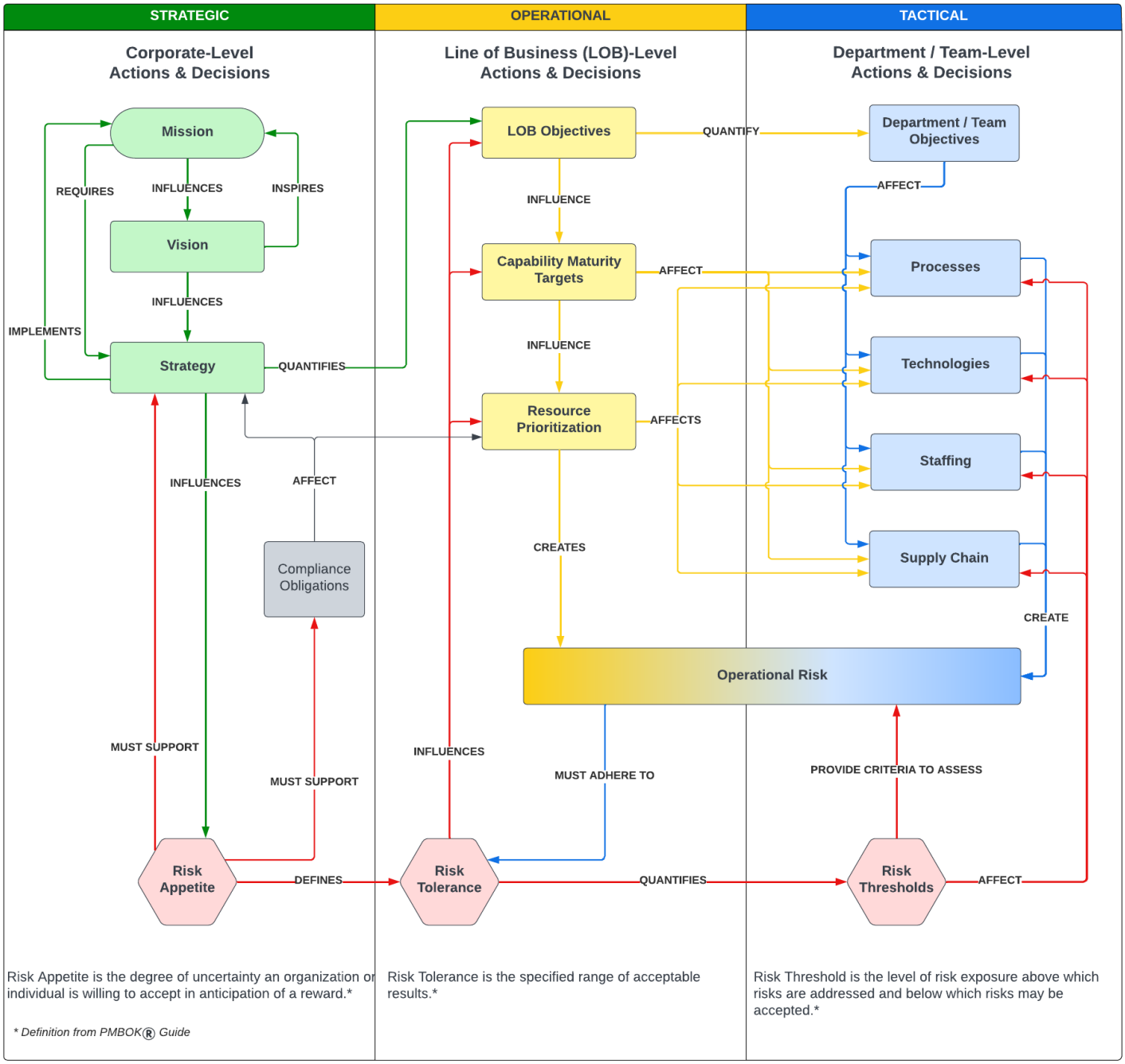
- Dispense with its long-standing risk appetite for this specific project so that a potentially lucrative business opportunity can exist?
- Is the AI project cancelled due to the level of risk?
- If the CEO/BoD proceeds with accepting the risk, is it violating its fiduciary duties, since it is accepting risk that it previously deemed unacceptable? Additionally, would it be considered negligent to accept high, severe or Extreme Risk (e.g., would a rational individual under similar circumstances make the same decision?)?

[8] *SEC - https://www.sec.gov/comments/265-24/26524-77.pdf*
[9] *IFRS - https://www.ifrs.org/content/dam/ifrs/project/definition-of-materiality/definition-of-material-feedback-statement.pdf*

SUMMARIZING THE INTEGRATION OF RISK MANAGEMENT & BUSINESS PLANNING

These key concepts of how risk appetite, risk tolerance and risk thresholds interact with strategic, operational and tactical actions and decisions can be visualized in the following graphic:[10]

- At the strategic layer, where corporate-level actions and decisions are made, the organization's risk appetite is defined. The scope of the risk appetite can be organization-wide or compartmentalized to provide enhanced granularity.
- At the operational level, where Line of Business (LOB)-level actions and decisions are made, the organization's risk tolerance is put into practice. The organization's risk tolerance is defined by its established risk appetite.
- At the tactical level, where department / team-level actions and decisions are made, the organization's risk thresholds are used to provide criteria to assess operational risk. That operational risk must adhere to the organization's risk tolerance and therefore, its risk appetite.



[10] *Strategic vs Operational vs Tactical Risk Management* - https://complianceforge.com/content/pdf/cybersecurity-practitioners-guide-to-risk-management.pdf

Risk Management: Strategic Considerations

At this level, corporate-level actions and decisions define the strategic direction of the organization and its approach to risk management practices:

Mission

- Influences the vision of the organization.
- Requires a strategy to accomplish.

Vision

- Inspires personnel to achieve the mission.

Strategy

- Implements the mission.
- Quantifies "downstream" objectives for Lines of Business (LOB)
- Influences the organization's risk appetite.

Compliance Obligations

- Affect the strategy.
- Affect resource prioritization.

Risk Appetite

- Must support the organization's strategy.
- Defines the organization's risk tolerance.

Risk Management: Operational Considerations

At this level, Line of Business (LOB)-level actions and decisions define the operational management of the organization:

Line of Business (LOB) Objectives

- Are quantified and prioritized by the organization's strategy.
- Influence necessary capability maturity targets.
- Quantifies "downstream" objectives at the department / team level.

Capability Maturity Targets

- Are influenced by LOB objectives.
- Influences resource prioritization.
- Affects:
    - Processes that are implemented to achieve objectives;
    - Technologies used to support operations;
    - Staffing levels at the department / team level; and
    - Supply chain quality & security (e.g., vendors, suppliers, contractors, consultants, etc.).

Resource Prioritization

- Creates operational risks.
- Affects:
    - Processes that are implemented to achieve objectives;
    - Technologies used to support operations;
    - Staffing levels at the department / team level; and
    - Supply chain quality & security (e.g., vendors, suppliers, contractors, consultants, etc.).

Risk Tolerance

- Is defined by the organization's risk appetite.
- Influences LOB objectives.
- Quantifies the organization's risk thresholds.

Risk Management: Tactical Considerations

At this level, department / team-level actions and decisions define the tactics used for day-to-day operations:

Department / Team Objectives

- Are quantified and prioritized by LOB objectives.
- Affect:
  - Processes that are implemented to achieve objectives;
  - Technologies used to support operations;
  - Staffing levels at the department / team level; and
  - Supply chain quality & security (e.g., vendors, suppliers, contractors, consultants, etc.).

Processes

- Are affected by:
  - Department / team objectives;
  - Capability maturity targets; and
  - Resource prioritization.
- Create operational risks.

Technologies

- Are affected by:
  - Department / team objectives;
  - Capability maturity targets; and
  - Resource prioritization.
- Create operational risks.

Staffing

- Are affected by:
  - Department / team objectives;
  - Capability maturity targets; and
  - Resource prioritization.
- Creates operational risks.

Supply Chain

- Are affected by:
  - Department / team objectives;
  - Capability maturity targets; and
  - Resource prioritization.
- Creates operational risks.

Risk Thresholds

- Provide criteria to assess operational risks.
- Affect:
  - Processes that are implemented to achieve objectives;
  - Technologies used to support operations;
  - Staffing levels at the department / team level; and
  - Supply chain quality & security (e.g., vendors, suppliers, contractors, consultants, etc.).

Operational Risk

- Is assessed against the organization's risk thresholds.
- Must adhere to the organization's risk tolerance, where the organization has four (4) options to address identified risks:
  1. Reduce the risk to an acceptable level;
  2. Avoid the risk;
  3. Transfer the risk to another party; or
  4. Accept the risk.

CYBERSECURITY & DATA PRIVACY RISK MANAGEMENT MODEL (C|P-RMM)

The concept of creating the C|P-RMM was to create an efficient methodology to identify, assess, report and mitigate risk. This project was approached from the perspective of asking the question, "*How should I management risk?*" and was a collaboration between ComplianceForge and the Secure Controls Framework (SCF).

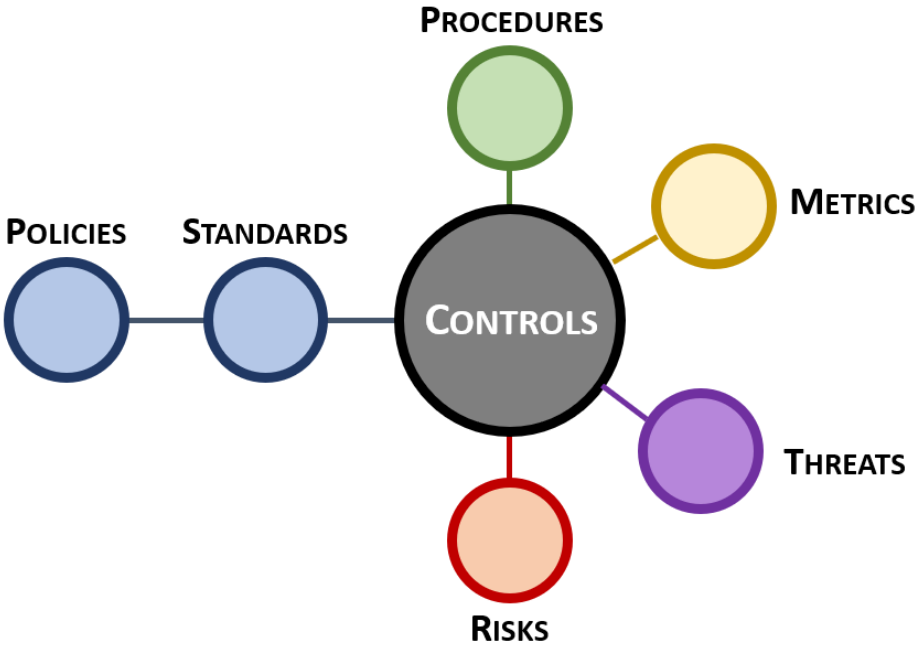
RISKS & THREATS DO NOT EXIST IN A VACUUM

Based on the applicable statutory, regulatory and contractual obligations that impact the scope of a risk assessment, an organization is expected to have an applicable set of cybersecurity and data privacy controls to cover those fundamental compliance obligations. That set of controls identifies the in-scope requirements that must be evaluated to determine what risk exists. This is generally considered to be a "gap assessment" where the assessor:

- Evaluates those controls based on the entity's Threat Catalog to identify current or potential control deficiencies; and
- Utilize the Risk Catalog to identify the applicable risks, based on the identified control deficiencies.

Therefore, it is vitally important to understand that risks and threats do not exist in a vacuum. If your cybersecurity and data privacy program is appropriately built, you will have a robust controls framework where risks and threats will map directly to controls. Why is this?

- Controls are central to managing risks, threats procedures and metrics.
- Risks, threats, metrics and procedures need to map into the controls, which then map to standards and policies.



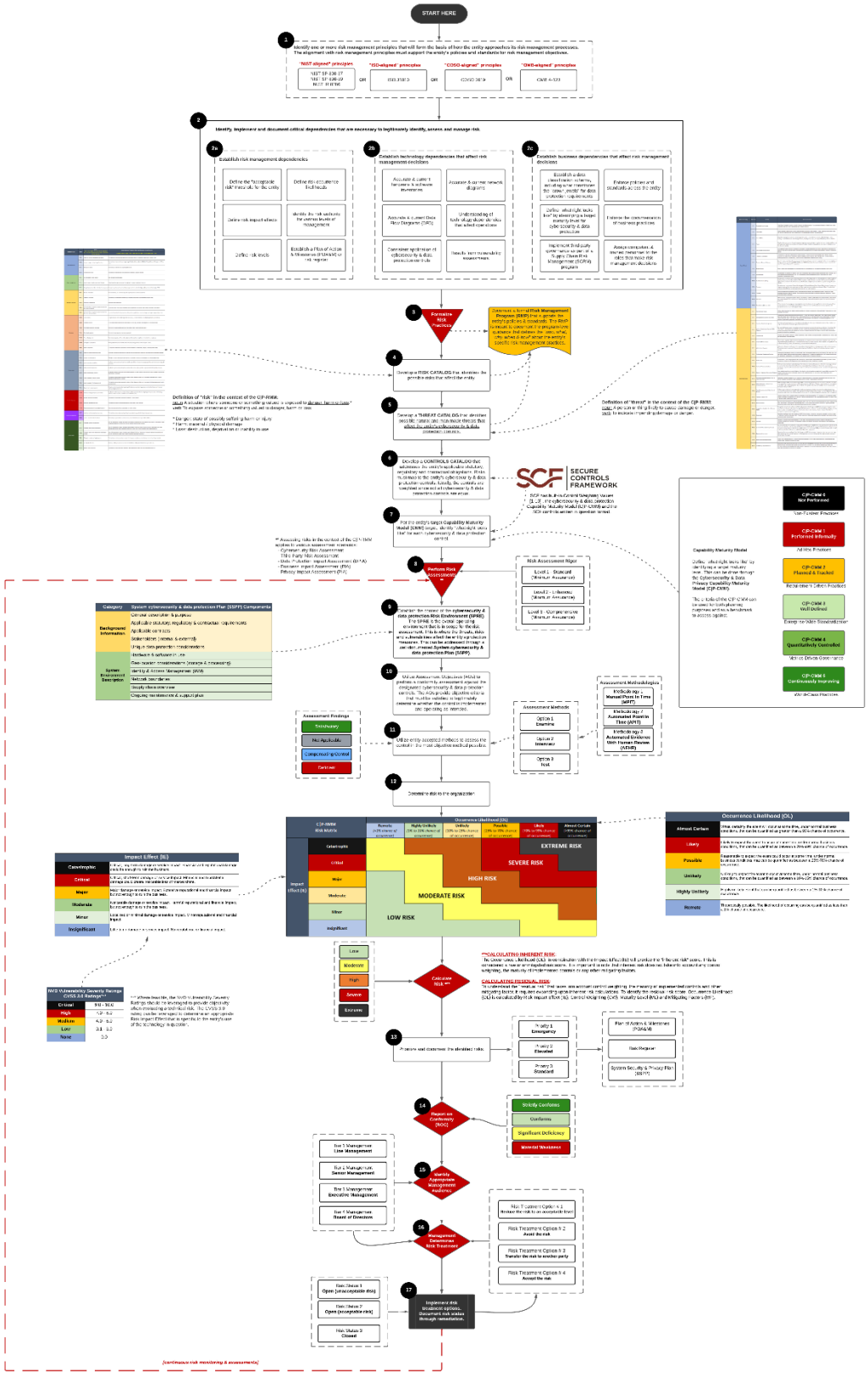
In risk management, the old adage is applicable that "the path to hell is paved with good intentions." Often, risk management personnel are tasked with creating risk assessments and questions to ask without having a centralized set of organization-wide cybersecurity and data privacy controls to work from. This generally leads to risk teams making up risks and asking questions that are not supported by the organization's policies and standards. For example, an organization is an "ISO shop" that operates an ISO 27002-based Information Security Management System (ISMS) to govern its policies and standards, but its risk team is asking questions about NIST SP 800-53 or NIST SP 800-171 controls that are not applicable to the organization.

This scenario of "making up risks" points to a few security program governance issues:

- If the need for additional controls to cover risks is legitimate, then the organization is improperly scoped and does not have the appropriate cybersecurity and data privacy controls to address its applicable statutory, regulatory, contractual or industry-expected practices.
- If the organization is properly scoped, then the risk team is essentially making up requirements that are not supported by the organization's policies and standards.

COVERAGE FROM START TO FINISH

The C|P-RMM addresses risk management from how you start building a risk management program through the ongoing risk management practices that are expected within your organization.



[image is downloadable from https://securecontrolsframework.com/content/SCF-Risk-Management-Model-Calculations.pdf]

C|P-RMM: Steps To Identify, Assess, Report & Mitigate Risk

The C|P-RMM is broken down into seventeen (17) core steps (note - these steps correspond to the diagram from the previous page):

1. Identify Risk Management Principles

It is necessary to identify one or more risk management principles that will form the basis of how the entity approaches its risk management processes. The alignment with risk management principles must support the entity's policies and standards for risk management objectives.

Common risk frameworks include:

- NIST SP 800-37
- ISO 31010
- COSO 2019
- OMB A-123

2. Identify, Implement & Document Critical Dependencies.

This is a multi-step process that involves identifying, implementing and documenting the critical dependencies that are necessary to legitimately identify, assess and manage risk:

2A. Risk Management Dependencies

It is vitally important to establish the fundamental risk management dependencies. These dependencies need to be standardized entity-wide or the organization will be hampered by conflicting definitions and expectations:

- Define the "acceptable risk" threshold for your entity.
- Define risk Occurrence Likelihood (OL).
- Define risk Impact Effect (IE).
- Define risk levels.
- Define the various levels of entity management who can "sign off" on risk levels.
- Establish a Plan of Action & Milestones (POA&M), risk register or some other method to track risks from identification through remediation.

2B. Technology Dependencies

In order to support risk management processes, it is necessary to establish the technology dependencies that affect risk management decisions:

- Maintain accurate and current hardware and software inventories.
- Maintain accurate and current network diagrams.
- Maintain accurate and current Data Flow Diagrams (DFD).
- Document the technology dependencies that affect operations (e.g., supporting systems, applications and services).
- Consistent application of cybersecurity and data privacy controls across the organization.
- Situational awareness of technology-related across the organization (e.g., vulnerability scanning & patch management levels).

2C. Business Dependencies

In order to support risk management processes, it is necessary to establish the business dependencies that affect risk management decisions:

- A data classification scheme needs to exist that is consistent across the organization, including an understanding of what constitutes the "crown jewels" of that require enhanced data protection requirements.
- Business leadership needs to dictate the technology support it requires for business operations to function properly. This enables technology and security leadership to define "what right looks like" from a necessary maturity level for cybersecurity and data privacy controls.
- A multi-discipline effort is needed to establish and maintain a Supply Chain Risk Management (SCRM) program that governs the organization's supply chain. This requires legal, procurement, security, privacy and Line of Business (LOB) involvement.
- Policies and standards must be uniformly applied across the organization.
- LOB management needs to ensure its project teams properly document business practices and provide that information to technology, cybersecurity and data privacy personnel in order to ensure a shared understanding of business practices

and requirements exists. This information is necessary to build out a System Security & Privacy Plan (SSPP).
- Since the LOB "owns" risk management decisions, the organization needs to ensure that those individuals in roles that make risk management decisions are competent and appropriately trained to make risk-related decisions.

3. Formalize Risk Management Practices

Document a formal Risk Management Program (RMP) that supports the entity's policies & standards. The RMP is meant to:

- Reference the most appropriate industry frameworks to provide a comprehensive and holistic approach to identifying, managing and remediating risks;
- Incorporate both cybersecurity and data privacy concepts in all stages of asset and data lifecycles; and
- Document the organization's program-level guidance that defines the "who, what, why, when & how" about the organization's specific risk management practices.

4. Establish A Risk Catalog

It is necessary to develop a risk catalog that identifies the possible risk(s) that affect the entity. The use case for the risk catalog is to identify the applicable risk(s) associated with a control deficiency. (*e.g., if the control fails, what risk(s) is the organization exposed to*?). In the context of the C|P-RMM, "risk" is defined as:

> *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.*

In the context of this definition of risk, it is important to define underlying components of this risk definition:

- *Danger: state of possibly suffering harm or injury*
- *Harm: material / physical damage*
- *Loss: destruction, deprivation or inability to use*

With this understanding of what risk is, the Secure Controls Framework (SCF) contains a catalog of thirty-nine (39) risks that are directly mapped to each of the SCF's controls.

Risk Grouping	Risk #	Risk* Note - Some of these risks may indicate a deficiency that could be considered a failure to meet "reasonable security practices"	Description of Possible Risk Due To Control Deficiency IF THE CONTROL FAILS, RISK THAT THE ORGANIZATION IS EXPOSED TO IS:
Access Control	R-AC-1	Inability to maintain individual accountability	The inability to maintain accountability (e.g., asset ownership, non-repudiation of actions or inactions, etc.).
	R-AC-2	Improper assignment of privileged functions	The inability to implement least privileges (e.g., Role-Based Access Control (RBAC), Privileged Account Management (PAM), etc.).
	R-AC-3	Privilege escalation	The inability to restrict access to privileged functions.
	R-AC-4	Unauthorized access	The inability to restrict access to only authorized individuals, groups or services.
Asset Management	R-AM-1	Lost, damaged or stolen asset(s)	Lost, damaged or stolen assets.
	R-AM-2	Loss of integrity through unauthorized changes	Unauthorized changes that corrupt the integrity of the system / application / service.

	R-AM-3	Emergent properties and/or unintended consequences	Emergent properties and/or unintended consequences from Artificial Intelligence & Autonomous Technologies (AAT).
Business Continuity	R-BC-1	Business interruption	Increased latency, or a service outage, that negatively impact business operations.
	R-BC-2	Data loss / corruption	The inability to maintain the confidentiality of the data (compromise) or prevent data corruption (loss).
	R-BC-3	Reduction in productivity	Diminished user productivity.
	R-BC-4	Information loss / corruption or system compromise due to technical attack	A technical attack that compromises data, systems, applications or services (e.g., malware, phishing, hacking, etc.).
	R-BC-5	Information loss / corruption or system compromise due to non-technical attack	A non-technical attack that compromises data, systems, applications or services (e.g., social engineering, sabotage, etc.).
Exposure	R-EX-1	Loss of revenue	A negative impact on the ability to generate revenue (e.g., a loss of clients or an inability to generate future revenue).
	R-EX-2	Cancelled contract	A cancelled contract with a client or other entity for cause (e.g., failure to fulfill obligations for secure practices).
	R-EX-3	Diminished competitive advantage	Diminished competitive advantage (e.g., lose market share, internal dysfunction, etc.).
	R-EX-4	Diminished reputation	Diminished brand value (e.g., tarnished reputation).
	R-EX-5	Fines and judgements	Financial damages due to fines and/or judgements from statutory / regulatory / contractual non-compliance.
	R-EX-6	Unmitigated vulnerabilities	Unmitigated technical vulnerabilities that lack compensating controls or other mitigation actions.
	R-EX-7	System compromise	A compromise of a system, application or service that affects confidentiality, integrity, availability and/or safety.
Governance	R-GV-1	Inability to support business processes	Insufficient cybersecurity and/or privacy practices that cannot securely support the organization's technologies & processes.

	R-GV-2	Incorrect controls scoping	Missing or incorrect cybersecurity and/or privacy controls due to incorrect or inadequate control scoping practices.
	R-GV-3	Lack of roles & responsibilities	Insufficient cybersecurity and/or privacy roles & responsibilities that cannot securely support the organization's technologies & processes.
	R-GV-4	Inadequate internal practices	Insufficient cybersecurity and/or privacy practices that can securely support the organization's technologies & processes.
	R-GV-5	Inadequate third-party practices	Insufficient Cybersecurity Supply Chain Risk Management (C-SCRM) practices that cannot securely support the organization's technologies & processes.
	R-GV-6	Lack of oversight of internal controls	The inability to demonstrate appropriate evidence of due diligence and due care in overseeing the organization's internal cybersecurity and/or privacy controls.
	R-GV-7	Lack of oversight of third-party controls	The inability to demonstrate appropriate evidence of due diligence and due care in overseeing third-party cybersecurity and/or privacy controls.
	R-GV-8	Illegal content or abusive action	Disruptive content or actions that negatively affect business operations (e.g., abusive content, harmful speech, threats of violence, illegal content, etc.).
Incident Response	R-IR-1	Inability to investigate / prosecute incidents	Insufficient incident response practices that prevent the organization from investigating and/or prosecuting incidents (e.g., chain of custody corruption, available sources of evidence, etc.).
	R-IR-2	Improper response to incidents	The inability to appropriately respond to incidents in a timely manner.
	R-IR-3	Ineffective remediation actions	The inability to ensure incident response actions were correct and/or effective.
	R-IR-4	Expense associated with managing a loss event	Financial repercussions from responding to an incident or loss.
Situational Awareness	R-SA-1	Inability to maintain situational awareness	The inability to detect cybersecurity and/or privacy incidents (e.g., a lack of situational awareness).
	R-SA-2	Lack of a security-minded workforce	The inability to appropriately educate and train personnel to foster a security-minded workforce.
Supply Chain	R-SC-1	Third-party cybersecurity exposure	Loss of Confidentiality, Integrity, Availability and/or Safety (CIAS) from third-party cybersecurity practices, vulnerabilities and/or incidents that affects the supply chain through impacted products and/or services.

	R-SC-2	Third-party physical security exposure	Loss of Confidentiality, Integrity, Availability and/or Safety (CIAS) from physical security exposure of third-party structures, facilities and/or other physical assets that affects the supply chain through impacted products and/or services.
	R-SC-3	Third-party supply chain relationships, visibility and controls	Loss of Confidentiality, Integrity, Availability and/or Safety (CIAS) from "downstream" third-party relationships, visibility and controls that affect the supply chain through impacted products and/or services.
	R-SC-4	Third-party compliance / legal exposure	The inability to maintain compliance due to third-party non-compliance, criminal acts, or other relevant legal action(s).
	R-SC-5	Use of product / service	The misuse of the product / service in a manner that it was not designed or how it was approved for use.
	R-SC-6	Reliance on the third-party	The inability to continue business operations, due to the reliance on the third-party product and/or service.

5. Establish A Threat Catalog

It is necessary to develop a threat catalog that identifies possible natural and man-made threats that affect the entity's cybersecurity & data 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 C|P-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:

5A. Natural Threats

Natural threats are caused by environmental phenomena that have the potential to impact individuals, processes, organizations or society, as a whole. The C|P-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.

5B. 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 C|P-RMM leverages a catalog of twenty-three (23) 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 of conventional explosive device with radioactive / chemical / biological material and be designed to scatter lethal and sub-lethal amounts of material over a wide area.
MT-5	Physical Crime	Physical crime includes "traditional" crimes of opportunity. These incidents can range from theft, to vandalism, riots, looting, arson and other forms of criminal activities.
MT-6	Terrorism & Armed Attacks	Armed attacks, regardless of the motivation of the attacker, can impact a business. Scenarios can range from single actors (e.g., "disgruntled" employee) all the way to a coordinated terrorist attack by multiple assailants. These incidents can range from the use of blade weapons (e.g., knives), blunt objects (e.g., clubs), to firearms and explosives.
MT-7	Utility Service Disruption	Utility service disruptions are focused on the sustained loss of electricity, Internet, natural gas, water, and/or sanitation services. These incidents can have a variety of causes but directly impact the fulfillment of utility services that your business needs to operate.
MT-8	Dysfunctional Management Practices	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 to (1) an absence of a required control or (2) a control deficiency.
MT-9	Human Error	Human error is a broad category that includes non-malicious actions that are unexpected and unpredictable by humans. These incidents can range from misconfigurations, to misunderstandings or other unintentional accidents.

MT-10	Technical / Mechanical Failure	Technical /mechanical failure is a broad category that includes non-malicious failure due to a defect in the technology, materials or workmanship. Technical / mechanical failures are unexpected and unpredictable, even when routine and preventative maintenance is performed. These incidents can range from malfunctions, to reliability concerns to catastrophic damage (including loss of life).
MT-11	Statutory / Regulatory / Contractual Obligation	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.
MT-12	Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) Data	Redundant, Obsolete/Outdated, Toxic or Trivial (ROTT) data is information an organization utilizes for business processes even though the data is untrustworthy, due to the data's currency, accuracy, integrity and/or applicability.
MT-13	Artificial Intelligence & Autonomous Technologies (AAT)	Artificial Intelligence & Autonomous Technologies (AAT) is a broad category that ranges from non-malicious failure due to a defect in the algorithm to emergent properties or unintended consequences. AAT failures can be due to hardware failures, inherent biases or other flaws in the underlying algorithm. These incidents can range from malfunctions, to reliability concerns to catastrophic damage (including loss of life).
MT-14	Fraud, Corruption and/or Willful Criminal Conduct	Willful criminal conduct is a broad category that includes consciously-committed criminal acts performed by individuals (e.g., mens rea). These incidents can include a wide-range of activities that includes fraud, corruption, theft and illegal content. Criminal conduct generally involves one of the following kinds of mens rea: (1) intent, (2) knowledge, (3) recklessness and/or (4) negligence.
MT-15	Conflict of Interest (COI)	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.
MT-16	Macroeconomics	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.
MT-17	Foreign Ownership, Control, or Influence (FOCI)	Foreign Ownership, Control, or Influence (FOCI) is a Supply Chain Risk Management (SCRM) threat category that pertains to the ownership of, control of, or influence over an organization. Primarily, the concern is if a foreign interest (e.g., foreign government or parties owned or controlled by a foreign government) has the direct or indirect ability to influence decisions that affect the management or operations of the organization.
MT-18	Geopolitical	Geopolitical is a Supply Chain Risk Management (SCRM) threat category that pertains to a specific geographic location, or region of relevance, that affects the supply chain. Primarily, the concern is if a foreign state can affect the supply chain through political intervention within the host nation.
MT-19	Sanctions	Sanctions is a Supply Chain Risk Management (SCRM) threat category that pertains to past or present fraudulent activity or corruption. Primarily, the concern is if the third-party is subject to suspension, exclusion or other sanctions that can affect the supply chain.
MT-20	Counterfeit / Non-Conforming Products	Counterfeit / Non-Conforming Products is a Supply Chain Risk Management (SCRM) threat category that pertains to the integrity of components within the supply chain. Counterfeits are products introduced to the supply chain that falsely claim to be produced by the legitimate Original Equipment Manufacturer (OEM), whereas non-conforming are OEM products / materials that fail to meet the customer specifications. Both can have a detrimental effect on the supply chain.

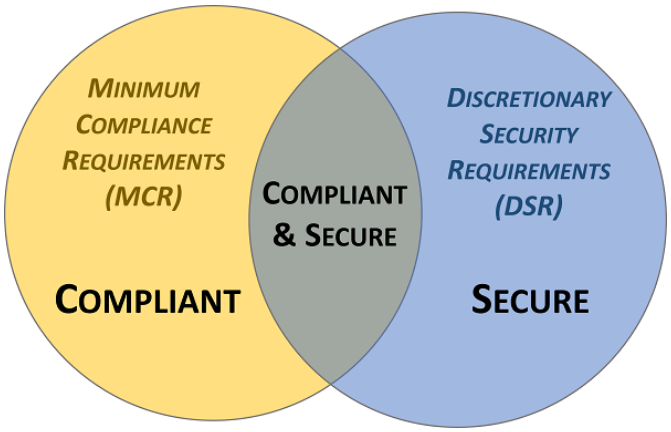
MT-21	Operational Environment	Operational Environment is a Supply Chain Risk Management (SCRM) threat category that pertains to the user environment (e.g., place of performance). Primarily, the concern is if the operational environment is hazardous that could expose the organization operationally or financially.
MT-22	Supply Chain Interdependencies	Supply Chain Interdependencies is a Supply Chain Risk Management (SCRM) threat category pertaining to interdependencies related to data, systems and mission functions.
MT-23	Third-Party Quality Deficiencies	Third-Party Quality Deficiencies is a Supply Chain Risk Management (SCRM) threat category that provide insights into the ability of the third-party to produce and deliver products and/or services as expected. This includes an understanding of the quality assurance practices associated with preventing mistakes or defects in manufactured/ developed products and avoiding problems when delivering solutions or services to customers.

6. Establish A Controls Catalog

It is necessary to develop a catalog of cybersecurity and data privacy controls that addresses the organization's applicable statutory, regulatory and contractual obligations. Risks used by the organization as part of risk analysis processes must map to the organization's existing cybersecurity & data privacy controls. Ideally, the controls are weighted since not all cybersecurity & data privacy controls are equal, in terms of impact or consequence.

To assist in this process, it is helpful for the organization to categorize its applicable controls according to "must have" vs "nice to have" requirements:[11]

- Minimum Compliance Requirements (MCR) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts.
- Discretionary Security Requirements (DSR) are tied to the organization's risk appetite since DSR are "above and beyond" MCR, where the organization self-identifies additional cybersecurity and data protection controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments.



Secure and compliant operations exist when both MCR and DSR are implemented and properly governed:

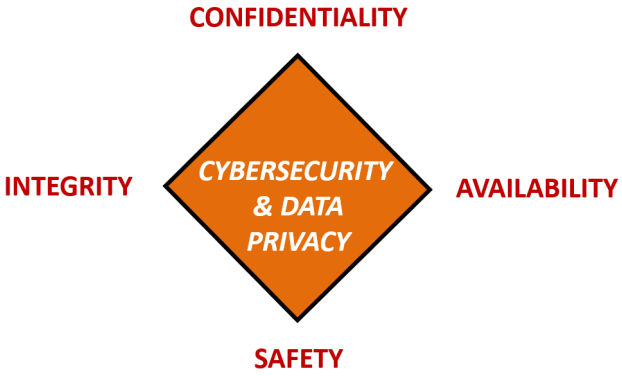
- MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCR establishes the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

The combination of MCR and DSR equate to an organization's Minimum Security Requirements (MSR), which define the "must have" and "nice to have" requirements for People, Processes, Technologies, Data & Facilities (PPTDFF) in one control set. It defines the Minimum Viable Product (MVP) technical and business requirements from a cybersecurity and data privacy perspective. In short, the MSR can be considered to be an organization's IT General Controls (ITGC), which establishes the basic controls that must be applied to systems, applications, services, processes and data throughout the enterprise. ITGC provides the foundation of assurance for an organization's decision makers. ITGC enables an organization's governance function to define how technologies are designed, implemented and operated.

Commensurate with risk, cybersecurity and data 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

[11] *Integrated Controls Management (ICM) model - https://complianceforge.com/content/pdf/complianceforge-integrated-controls-management.pdf*

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 (CIAS):



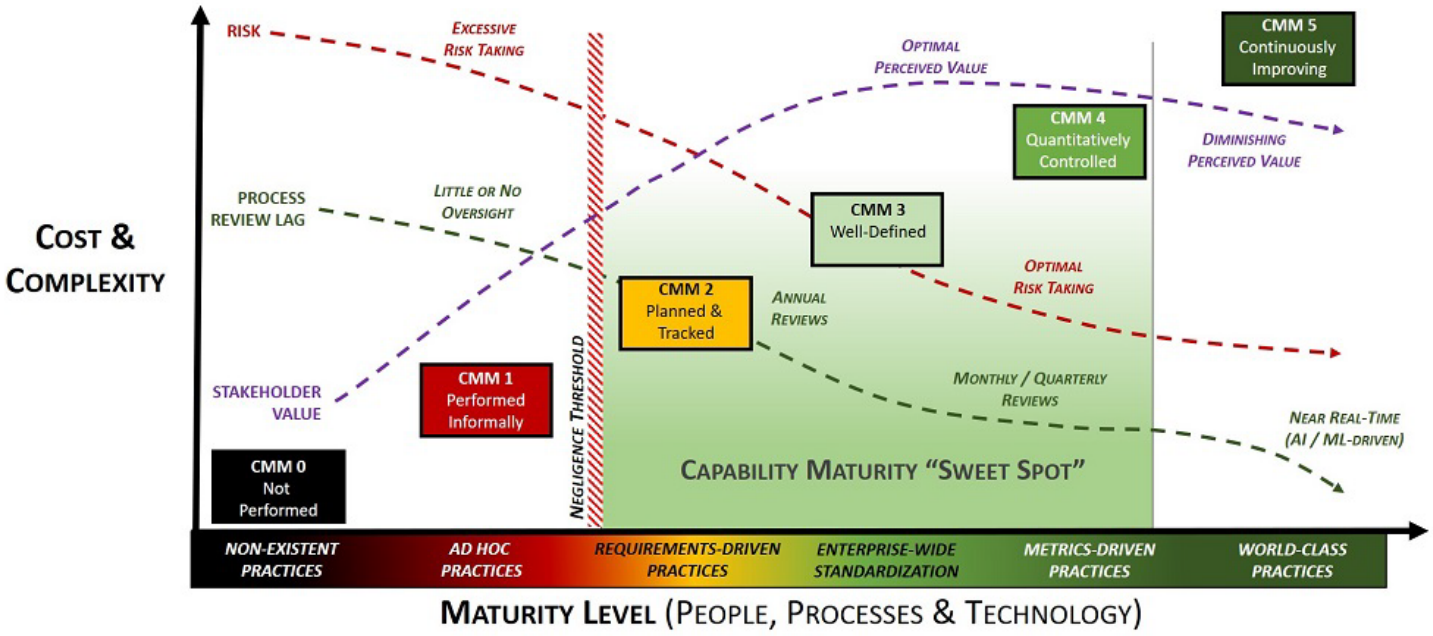
- **Confidentiality** – Confidentiality addresses preserving restrictions on information access and disclosure so that access is limited to only authorized users and services.
- **Integrity** – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and 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.

Note: The SCF has built-In Control Weighting Values [1-10], a maturity model and the SCF controls written in question format.

7. Define Capability Maturity Model (CMM) Targets

It is necessary for an entity to define "what right looks like" for the level of maturity it expects for deployed cybersecurity and data privacy controls. This is generally defined by aligning with a Capability Maturity Model (CMM). While there are several to choose from, the SCF's **Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM)** contains control-level criteria for each of the levels of the maturity model.[12]

Maturity model criteria should be used by the organization as the benchmark to evaluate cybersecurity and data privacy controls.



8. Define Assessment Rigor

With the previous steps addressed, an assessor will leverage those deliverables (e.g., Risk Management Program (RMP), threat catalog, risk catalog, controls catalogs, etc.) to implement a functional capability to assess risk across the entity. That documented assessment criteria from the previous steps exist to guide the assessor when performing risk assessments.

[12] *SCF Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM) - https://securecontrolsframework.com/content/SCF-Capability-Maturity-Model.pdf*

This risk assessment approach applies to various assessment scenarios:

- Cybersecurity Risk Assessment;
- Third-Party Risk Assessment;
- Data Protection Impact Assessment (DPIA);
- Business Impact Assessment (BIA); and
- Privacy Impact Assessment (PIA).

There are three (3) levels of rigor for a risk assessment:

1. Standard;
2. Enhanced; and
3. Comprehensive.

The definition of each assessment method includes types of objects to which the method can be applied. In addition, the application of each method is described in terms of the attributes of depth and coverage.

- The depth attribute addresses the rigor and level of detail of the assessment.
- The coverage attribute addresses the scope or breadth of the assessment.

8A. Risk Assessment Level 1: Standard Rigor (Minimum Assurance)

Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:

1. Implemented; and
2. Free of obvious errors.

Standard rigor represents sufficient due care in the evaluation of cybersecurity and/or data protection controls. Standard rigor is appropriate for the Manual Point In Time (MPIT) assessment methodology that:

1. Is relevant to a specific point in time (time at which the controls were evaluated); and
2. Relies on the manual review of artifacts to derive a finding.

8B. Risk Assessment Level 2: Enhanced Rigor (Moderate Assurance)

Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:

1. The applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors; and
2. There are increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended.

Enhanced rigor is appropriate for the Automated Point In Time (APIT) assessment methodology that utilizes automation to augment a traditional assessment methodology, where Artificial Intelligence and Autonomous Technologies (AAT) are used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

1. Is relevant to a specific point in time (time at which the controls were evaluated);
2. In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
3. The combined output of automated and manual reviews of artifacts is used to derive a finding.

8C. Risk Assessment Level 3: Comprehensive Rigor (High Assurance)

Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:

1. Whether the applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors;
2. Whether there are further increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended on an ongoing and consistent basis; and

3. There is support for continuous improvement in the effectiveness of the applicable controls.

Comprehensive rigor is appropriate for the Automated Evidence with Human Review (AEHR) assessment methodology that is used for ongoing, continuous control assessments:

1. AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
2. Recurring human reviews:
    a. Evaluate the legitimacy of the results from automated control assessments; and
    b. Validate the automated evidence review process to derive a finding.

9. Establish The Context For Assessing Risks

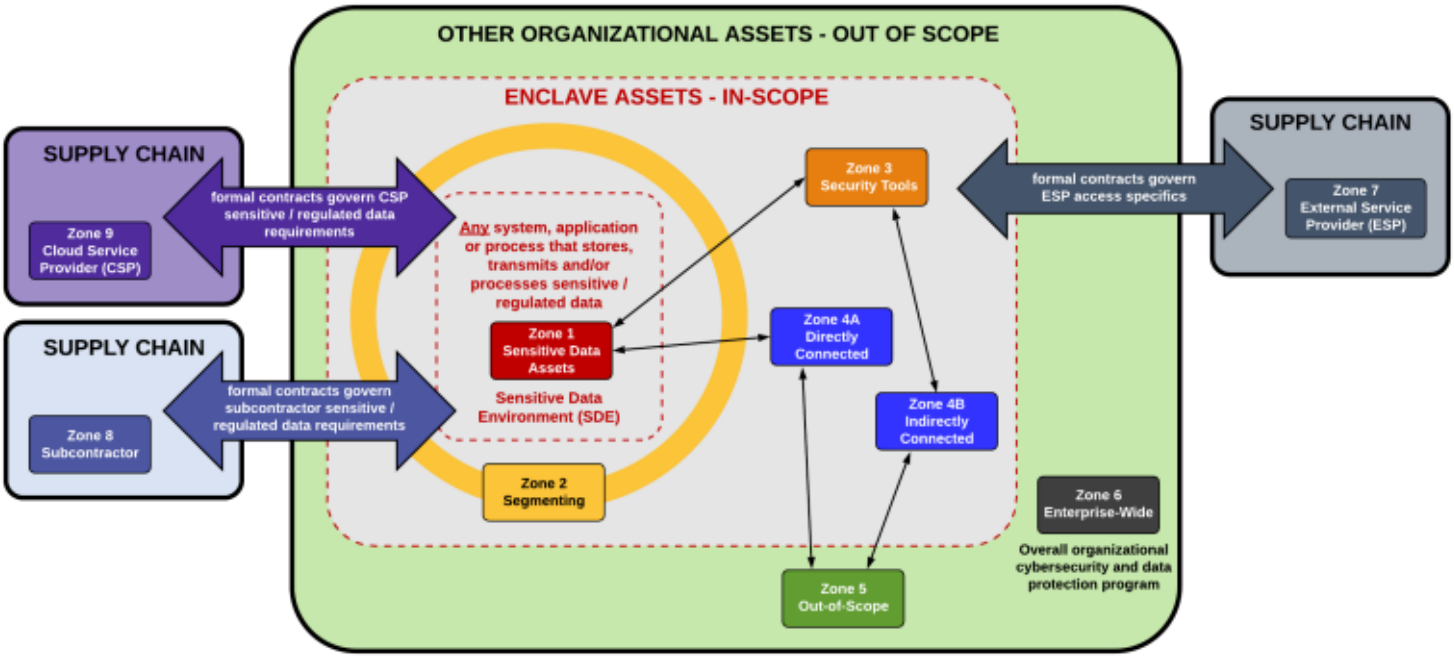
Now that a methodology exists to assess risk, it is necessary for the assessor to establish the context of the Cybersecurity & Data Privacy Risk Environment (SPRE). The SPRE is the overall operating environment that is in scope for the risk assessment. This is where applicable threats, risks and vulnerabilities affect the entity's protection measures.

An assessor can generally find this information in a well-documented System Security & Privacy Plan (SSPP). If the scoping is incorrect, the context will likely also be incorrect, which can lead to a misguided and inaccurate risk assessment.

SPRE Context	SSPP Component
Background Information	General description & purpose
	Applicable statutory, regulatory & contractual requirements
	Applicable contracts
	Stakeholders (internal & external)
	Unique data protection considerations
System Environment Description	Hardware & software in use
	Geolocation considerations
	Identity & Access Management (IAM)
	Network boundaries
	Supply chain overview
	Ongoing maintenance & support plan

Without specific statutory, regulatory or contractual scoping instructions, the organization should leverage the Unified Scoping Guide (USG) as the basis for scoping sensitive and/or regulated data.[13]

[13] *Unified Scoping Guide (USG) - https://complianceforge.com/content/pdf/unified-scoping-guide-usg.pdf*



10. Conformity Assessment (Controls Gap Assessment)

Based on the applicable statutory, regulatory and contractual obligations that impact the SPRE, the entity is expected to have an applicable set of controls to cover those needs. That set of controls identifies the in-scope requirements that must be evaluated to determine the organization's conformity against that specified control set.

The assessor leverages Assessment Objectives (AOs) to perform a conformity assessment against the designated cybersecurity & data protection controls. The AOs provide objective criteria that must be satisfied to legitimately determine whether the control is implemented and operating as intended.

Note: There may be multiple AOs associated with a control. The SCF spreadsheet contains an AO catalog, tied to SCF controls.

11. Control Assessment Methods & Findings

The process of assessing controls (including AOs) involves determining the most appropriate assessment method, the methodology that will be used to assess controls and a way to report on the resulting findings. This section covers those topics.

11A. Assessment Methods

Assessors are expected to review artifacts and other evidence to independently verify that an organization meets the AO for all applicable controls. There are three (3) assessment methods:

1. Examine;
2. Interview; and
3. Test.

11A-1. Examine

The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.

11A-2. Interview

The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.

11A-3. TEST

The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.

When the control deficiencies are identified, the assessor must utilize an entity-accepted method to assess the risk in the most objective method possible. Criteria for assessing a control for deficiencies is generally defined as either:

- Qualitative;
- Semi-Qualitative; or
- Quantitative

In most cases, it is not feasible to have an entirely quantitative assessment, so assessments should be expected to include semi-qualitative or qualitative aspects. There are multiple methods to actually assess and calculate risk. The C|P-RMM simplifies risk management practices by utilizing a form of risk matrix that takes Occurrence Likelihood (OL) and Impact Effect (IE) into account to determine the risk categorization.

11B. METHODOLOGIES

There are three (3) options to implement assessment methods:

1. Manual Point In Time (MPIT);
2. Automated Point In Time (APIT); and
3. Automated Evidence with Human Review (AEHR).

11B-1. MANUAL POINT IN TIME (MPIT)

MPIT is a traditional assessment methodology that:

- Is relevant to a specific point in time (time at which the controls were evaluated); and
- Relies on the manual review of artifacts to derive a finding;

11B-2. AUTOMATED POINT IN TIME (APIT)

APIT utilizes automation to augment a traditional assessment methodology, where Artificial Intelligence and Autonomous Technologies (AAT) are used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

- Is relevant to a specific point in time (time at which the controls were evaluated);
- In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
- The combined output of automated and manual reviews of artifacts is used to derive a finding; or

11B-3. AUTOMATED EVIDENCE WITH HUMAN REVIEW (AEHR)

AEHR is used for ongoing, continuous control assessments:

- AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
- Recurring human reviews:
  - Evaluate the legitimacy of the results from automated control assessments; and
  - Validate the automated evidence review process to derive a finding.

11C. ASSESSMENT FINDINGS

When a control is assessed, the result is referred to as a finding. Findings are not designed to have a specific "score" associated with the evaluation of a control. Its value is in the subjective status associated with the implementation of the control. These findings are useful for the Report on Conformity (ROC), or whatever you want to call the risk assessment report, to summarize the findings to the organization's management.

The four (4) categories of findings are:

1. Satisfactory;
2. Not Applicable;
3. Compensating Control; and
4. Deficient.

11C-1. SATISFACTORY

Positive finding. Appropriate evidence of due diligence and due care exists to demonstrate the design and/or operation of an organization's cybersecurity and/or data protection control satisfactorily meets all applicable Assessment Objectives (AOs) that

determine if the intent of the control is achieved.

11C-2. Not Applicable

Neutral finding. Appropriate evidence demonstrates the control is not applicable, due to applicable business practices and/or technical implementation.

11C-3. Compensating Control

Positive finding. Appropriate evidence of due diligence and due care exists to demonstrate the design and/or operation of an organization's cybersecurity and/or data protection control satisfactorily meets all applicable AOs that determine if the intent of the control is achieved.

11C-4. Deficient

Negative finding. A "deficiency" exists when the design and/or operation of an organization's cybersecurity and/or data protection control fails to meet one of more AO that determines if the intent of the control is achieved.

12. Determine Risk Exposure

Based on deficient controls identified in the previous step, it is necessary to determine the organization's exposure to risk, since the control deficiency(ies) creates risk (e.g., a situation where someone or something valued is exposed to danger, harm or loss).

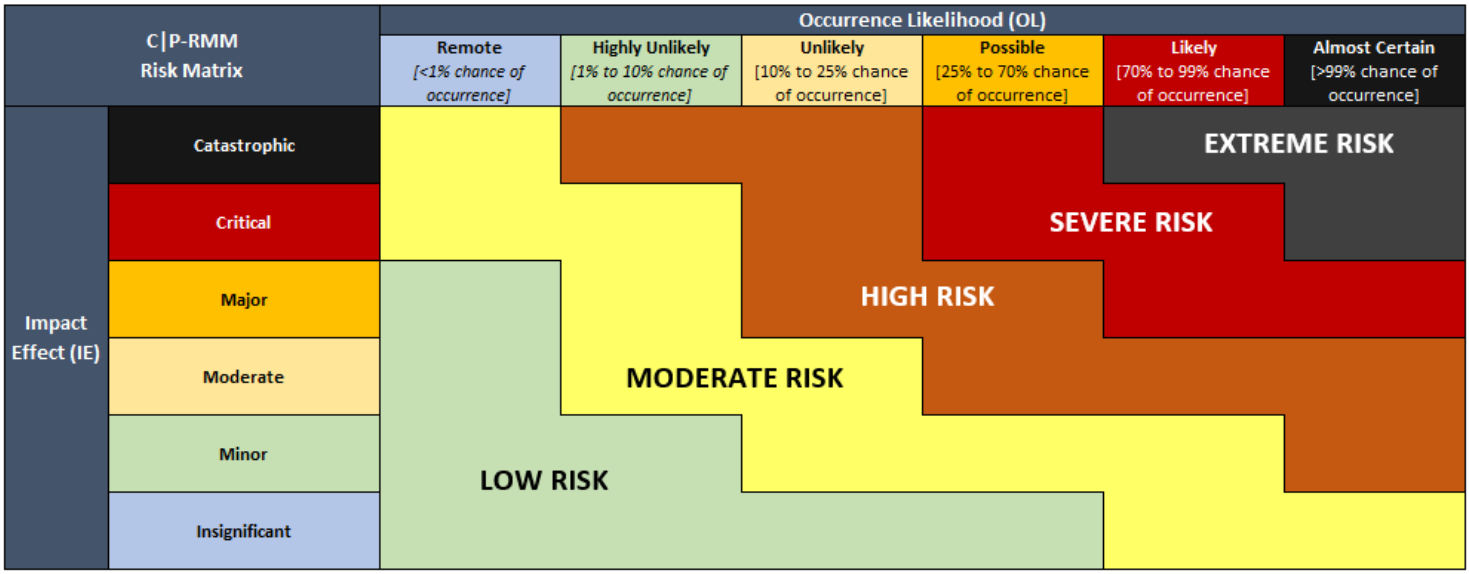
Note: Determining risk exposure can be calculated at an individual level and averaged across multiple deficiencies.

The C|P-RMM leverages the following five (5) categories of risk:

1. Low;
2. Moderate;
3. High;
4. Severe; and
5. Extreme.

These categories of risk are determined through an intersection of:

1. Impact Effect (IE); and
2. Occurrence Likelihood (OL)



12A. Impact Effect (IE)

The six (6) categories of IE are:

1. Insignificant *(e.g., organization-defined little-to-no impact to business operations);*
2. Minor *(e.g., organization-defined minor impacts to business operations)*;
3. Moderate *(e.g., organization-defined moderate impacts to business operations)*;
4. Major *(e.g., organization-defined major impacts to business operations)*;

5. Critical *(e.g., organization-defined critical impacts to business operations)*; and
6. Catastrophic *(e.g., organization-defined catastrophic impacts to business operations).*

12B. Occurrence Likelihood (OL)

The six (6) categories of OL are:

1. Remote possibility *(e.g., <1% chance of occurrence)*;
2. Highly unlikely *(e.g., from 1% to 10% chance of occurrence)*;
3. Unlikely *(e.g., from 10% to 25% chance of occurrence)*;
4. Possible *(e.g., from 25% to 70% chance of occurrence)*;
5. Likely *(e.g., from 70% to 99% chance of occurrence)*; and
6. Almost certain *(e.g., >99% chance of occurrence)*.

There are three (3) general approaches are commonly employed to estimate OL:

1. Relevant historical data;
2. Probability forecasts; and
3. Expert opinion.

12C. Inherent Risk

From the risk assessment matrix, the intersection between OL and IE will provide the inherent ris" score. This is considered a raw or unmitigated risk score. It is important to note that inherent risk does not take into account any control weighting, the maturity of implemented controls or any other mitigating factors.

12D. Residual Risk

Residual risk takes into account control weighting, the maturity of implemented controls and other mitigating factors where it builds upon the inherent risk calculation. To identify the residual risk score, OL is calculated by IE, Control Weighting (CW), Maturity Level (ML) and Mitigating Factors (MF). See Appendix A for more details on calculating residual risk.

13. Prioritize & Document Identified Deficiencies

Once a deficiency with a control is identified, it is necessary to determine the level of urgency that should be applied to it. Findings need to be categorized by one of the following levels of prioritization:

- Emergency;
- Elevated; or
- Standard.

The organization's risk documentation methodology should utilize one or more of the following options:

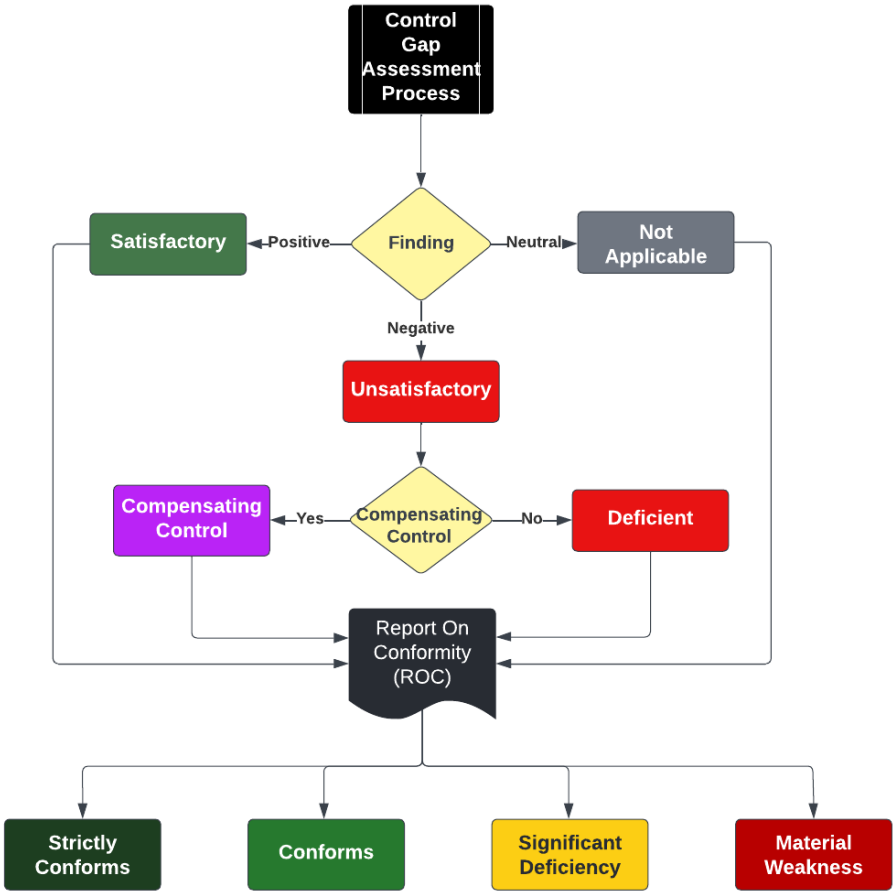
- Risk Register
- Plan of Action & Milestones (POA&M)
- Risk Assessment Report
- System Security & Privacy Plan (SSPP); or
- Another documentation option of your choosing.

14. Risk Determination: Report on Conformity (ROC)

Risk management requires educating stakeholders for situational awareness and decision-making purposes. There are many options and formats available to report, but this can be considered a Report on Conformity (ROC). The reason for this is a risk assessment fundamentally is evaluating if an organization's cybersecurity and data privacy practices support its stated risk tolerance.

This approach can be summarized by reporting to the organization's management on the "health" of the assessed controls by one of the following four (4) risk determinations:

1. Strictly Conforms;
2. Conforms;
3. Significant Deficiency; and
4. Material Weakness.



14A. *Strictly Conforms*

This is a positive outcome and indicates that at a high-level, the organization's cybersecurity and data privacy practices conform to its selected cybersecurity and data privacy practices. Strictly Conforms means:

- The organization/LOB can demonstrate Strict Conformity with its selected cybersecurity and/or data protection controls, where one hundred percent (100%) of the assessed controls have reasonable evidence to conclude:
  - The controls are met and operational;
  - Any control designated as Not Applicable (N/A) is validated as such by the assessor; and/or
  - Where applicable, compensating controls are validated by the assessor as being:
    - Applicable;
    - Reasonable; and
    - Implemented and operating properly; and
- Assessed controls provide reasonable assurance that the organization's/LOB's cybersecurity and data protection program provides adequate security, where it:
  - Adheres to a defined and documented risk tolerance;
  - Mitigates material cybersecurity and/or data protection risks;
  - Is designed to detect and protect against material cybersecurity and/or data protection threats; and
  - Is prepared to respond to material incidents.

Strictly Conforms is a statement to the organization's management that sufficient evidence of due care and due diligence exists to assure that the organization's stated risk tolerance can be achieved.

14B. *Conforms*

This is a positive outcome and indicates that at a high-level, the organization's cybersecurity and data privacy practices conform to its selected cybersecurity and data privacy practices. Conforms means:

- The organization/LOB can demonstrate Conformity with its selected cybersecurity and/or data protection controls, where at least eighty percent (80%) of the assessed controls have reasonable evidence to conclude:
  - The controls are met and operational;
  - Any control designated as Not Applicable (N/A) is validated as such by the assessor; and/or

    - Where applicable, compensating controls are validated by the assessor as being:
        - Applicable;
        - Reasonable; and
        - Implemented and operating properly; and
- Any assessed control deficiency is not material to the organization's/LOB's cybersecurity and data protection program; and
- Assessed controls provide reasonable assurance that the organization's/LOB's cybersecurity and data protection program provides adequate security, where it:
    - Adheres to a defined and documented risk tolerance;
    - Mitigates material cybersecurity and/or data protection risks;
    - Is designed to detect and protect against material cybersecurity and/or data protection threats; and
    - Is prepared to respond to material incidents.

Conforms is a statement to the organization's management that sufficient evidence of due care and due diligence exists to assure that the organization's stated risk tolerance can be achieved.

14C. Significant Deficiency

This is a negative outcome and indicates the organization was unable to demonstrate conformity with its selected cybersecurity and data privacy practices, due to systematic problems. Significant Deficiency means:

- The organization/LOB can demonstrate limited conformity with its selected cybersecurity and/or data protection controls due to a systemic problem within the organization's cybersecurity and data protection program, where:
    - At least seventy percent (70%), but less than eighty percent (80%), of the assessed controls have reasonable evidence to conclude:
        - The controls are met and operational;
        - Any control designated as N/A is validated as such by the assessor; and/or
        - Where applicable, compensating controls are validated by the assessor as being:
            - Applicable;
            - Reasonable; and
            - Implemented and operating properly;
- Any assessed control deficiency is not material to the organization's cybersecurity and data protection program;
- Assessed controls do not provide reasonable assurance that the organization's cybersecurity and data protection program provides adequate security, where it:
    - Adheres to a defined and documented risk tolerance;
    - Mitigates material cybersecurity and/or data protection risks;
    - Is designed to detect and protect against material cybersecurity and/or data protection threats; and
    - Is prepared to respond to material incidents; and
- The organization's cybersecurity and data protection program:
    - Has systemic problems inherent in the overall function of a team, department, project, application, service and/or vendor rather than a specific, isolated factor; and
    - Requires implementing limited changes to personnel, technology and/or practices to correct the design and implementation of deficient cybersecurity and/or data protection controls.

Significant Deficiency is a statement to the organization's management that insufficient evidence of due care and due diligence exists to assure that the organization's stated risk tolerance is achieved, due to a systemic problem in the cybersecurity and/or privacy program.

In the context of a significant deficiency, a systemic problem is a consequence of issues inherent in the overall function (e.g., team, department, project, application, service, vendor, etc.), rather than a specific, isolated factor. Systemic errors may require changing the structure, personnel, technology and/or practices to remediate the significant deficiency.

14D. Material Weakness

This is a negative outcome and indicates the organization is unable to demonstrate conformity with its selected cybersecurity and data privacy practices, due to deficiencies that make it probable that reasonable-expected threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance that the organization can adhere to its stated risk tolerance. Material Weakness means:

- The organization/LOB cannot demonstrate conformity with its selected cybersecurity and/or data protection controls due

to deficiencies that make it probable that reasonably expected threats will not be promptly detected or prevented, where:
    - One (1), or more, material controls is/are deficient; and/or
    - Less than seventy percent (70%) of the assessed controls have reasonable evidence to conclude:
        - The controls are met and operational;
        - Any control designated as N/A is validated by the assessor and confirmed as such; and/or
        - Where applicable, compensating controls are validated by the assessor as being:
            - Applicable;
            - Reasonable; and
            - Implemented and operating properly;
- Assessed controls do not provide reasonable assurance that the organization's cybersecurity and data protection program adequately:
    - Adheres to a defined and documented risk tolerance;
    - Mitigates material cybersecurity and/or data protection risks; and/or
    - Possesses the capability to:
        - Detect and protect against material cybersecurity and/or data protection threats; and/or
        - Respond to material incidents; and
- The organization's cybersecurity and data protection program:
    - Cannot perform its stated mission; and
    - Drastic changes to people, processes and/or technologies are required to remediate the deficiencies.

Material Weakness is a statement to the organization's management that (1) the cybersecurity and/or privacy program is incapable of successfully performing its stated mission and (2) drastic changes to people, processes and/or technology are necessary to remediate the findings.

15. Identify The Appropriate Management Audience

It is critically important that as part of an entity's program to manage risk that various levels of management are identified with varying authority, each with a pre-described ability to make risk management decisions. This helps prevent low-level managers from recklessly accepting risks that should be reserved for more senior management. A common tiered structure for risk management decisions includes:

- Line Management;
- Senior Management;
- Executive Management; and
- Board of Directors.

The organization's RMP defines the specific risk authority that roles have to make risk management decisions.

16. Management Determines Risk Treatment

Risk management is a management decision:

- Cybersecurity and IT generally do not "own" identified risk.
- The ultimate responsibility is on the management structure of the team/department/LOB that "owns" the business process or technology that is in use.

Common risk treatment options available to an organization's management team include:

- Reducing the risk to an acceptable level;
- Avoiding the risk;
- Transferring the risk to another party (e.g., insurance, outsourcing, etc.); and
- Accepting the risk.

17. Cybersecurity & Data Protection Practitioners Implement & Document Risk Treatment

When managing risk, it should be kept as simple as possible. Realistically, risk treatment is either "open" or "closed" but it can sometimes be useful to provide more granularity into open items to assist in reporting on risk management activities:

- Open (unacceptable risk);
- Open (acceptable risk); and
- Closed.

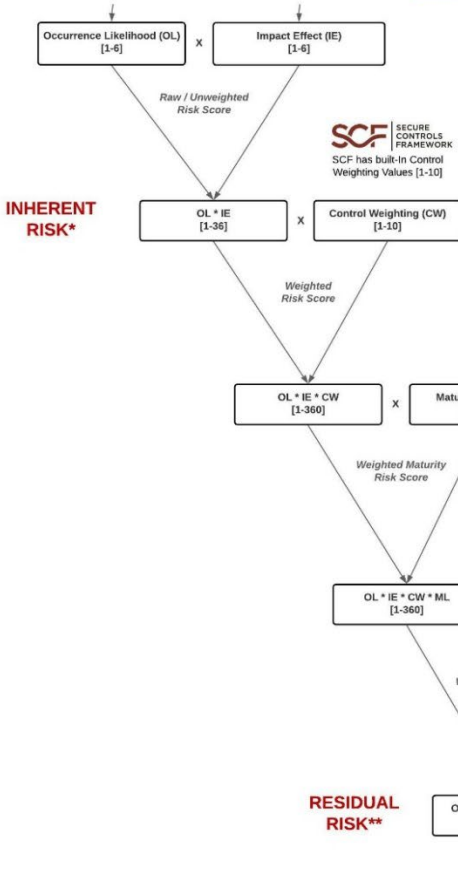
APPENDIX A: CALCULATING INHERENT RISK VS RESIDUAL RISK

It is possible to use a straightforward method to calculate risk using C|P-RMM. Both Inherent Risk & Residual Risk map into the C|P-RMM Risk Matrix (graphic shown below):

- For Inherent Risk, find the cell where Occurrence Likelihood (OL) intersects Impact Effect (IE) to determine the risk level.
- For Residual Risk, utilize the calculated Residual Risk values to determine the corresponding risk level.

Occurrence Likelihood (OL)	Score	Description
Almost Certain	6	Virtual certainty the event will occur at some time, under normal business conditions, that can be quantified as greater than a 99% chance of occurrence.
Likely	5	Likely to expect the event to occur at some time, under normal business conditions, that can be quantified as between a 70%-99% chance of occurrence.
Possible	4	Reasonable to expect the event could occur at some time, under normal business conditions, that can be quantified as between a 25%-70% chance of occurrence.
Unlikely	3	Unlikely to expect the event to occur at some time, under normal business conditions, that can be quantified as between a 10%-25% chance of occurrence.
Highly Unlikely	2	Highly-unlikely event that can be quantified as between a 1%-10% chance of occurrence.
Remote	1	Theoretically possible. The likelihood of occurring can be quantified as less than a 1% chance of occurrence.

Impact Effect (IE)	Score	Description
Catastrophic	6	Critical, long-term damage or service impact. Financial and reputational damage could be enough to ruin the business.
Critical	5	Critical, short-term damage or service impact. Financial and reputational damage could create noticeable loss of market share.
Major	4	Major damage or service impact. Extensive reputational and financial impact, but not enough to ruin the business.
Moderate	3	Noticeable damage or service impact. Harmful reputational and financial impact, but not enough to ruin the business.
Minor	2	Localized or minimal damage or service impact. Minor reputational and financial impact.
Insignificant	1	Little to no damage or service impact. No reputational or financial impact.



CALCULATING INHERENT RISK: *[OL * IE]*

The Occurrence Likelihood (OL), in combination with the Impact Effect (IE) will provide the "inherent risk" score.

Note - Inherent risk does not take into account any control weighting, the maturity of implemented controls or any other mitigating factors.

CALCULATING RESIDUAL RISK: *[OL* IE * CW * ML * MF]*

To understand the "residual risk" that takes into account control weighting, the maturity of implemented controls and other mitigating factor, it requires expanding upon inherent risk calculations.

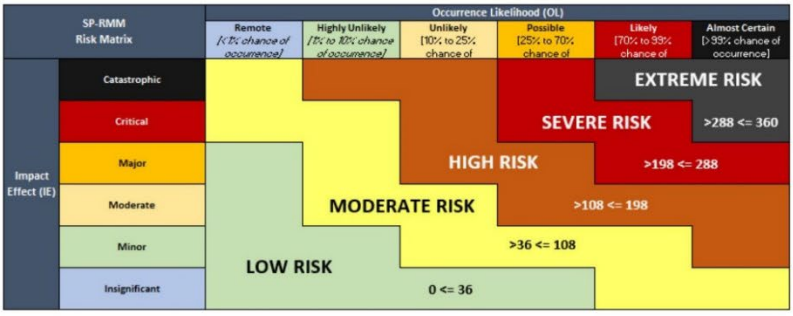
To identify the residual risk score, Occurrence Likelihood (OL) is calculated by Risk Impact Effect (IE), Control Weighting (CW), Maturity Level (ML) and Mitigating Factors (MF).

Maturity Level (ML)	ML Description	ML Value
0	Not Performed	1.0
1	Performed Informally	1.0
2	Planned & Tracked	0.9
3	Well Defined	0.7
4	Quantitatively Controlled	0.6
5	Continuously Improving	0.5

Mitigating Factor (MF)	Risk Reduction	MF Value
N/A - Not Required	Not Applicable	1.0
No Mitigating Factors Available	0%	1.0
Minimal Impact Reduction (Occurrence and/or Impact)	10%	0.9
Moderate Impact Reduction (Occurrence and/or Impact)	30%	0.7
Significant Impact Reduction (Occurrence and/or Impact)	50%	0.5

Risk Level	Residual Risk Values
Low	1 <= 36
Moderate	>36 <= 108
High	>108 <= 198
Severe	>198 <= 288
Extreme	>288 <= 360

Both **Inherent Risk** & **Residual Risk** map into the **SP-RMM Risk Matrix** (graphic shown below.
- For Inherent Risk, find the cell where Occurrence Likelihood (OL) intersects Impact Effect (IE) to determine the risk level.
- For Residual Risk, utilize the calculated Residual Risk values (see chart above) to determine the corresponding risk level.



https://securecontrolsframework.com/content/SCF-Risk-Management-Model-Calculations.pdf

Step 1: Calculate The Inherent Risk

To determine the inherent risk, calculate the Occurrent Likelihood (OL) by the Impact Effect (IE).

Step 2: Account For Control Weighting

Not all cybersecurity and data privacy controls are equal, so it is important to apply weighting to the importance of controls. The SCF contains pre-defined control weightings that can be edited for an entity's unique requirements. This Control Weighting (CW) is multiplied by the inherent risk score from Step 1.

Step 3: Account For Maturity Level Targets

The next step is meant to determine a weighted maturity score that takes control maturity into account. The more mature a control is, the greater the risk should be reduced. Maturity Level (ML) is multiplied by the value determined in Step 2.

Step 4: Account For Mitigating Factors To Determine Residual Risk

The final step is to account for Mitigating Factors (MF), which can be compensating controls or other process/technology considerations that mitigate risk, specific to the identified threats.

The end calculation to determine residual risk is: **OL * IE * CW * ML * MF**

Leveraging the by ComplianceForge's Risk Management Program (RMP) structure, it is straightforward to translate the calculated value of the residual risk score into a user-friendly risk category:

Risk Category	Range
Low	0 <= 36
Moderate	>36 <= 108
High	>108 <= 198
Severe	>198 <= 288
Extreme	>288 <= 360

APPENDIX B: REPORTING RISK FINDINGS: APPLYING THE CONCEPTS OF ASSURANCE, CONFORMITY & MATERIALITY

The concepts of assurance, conformity and materiality are integral into meaningful risk management decisions.

NIST defines assurance as, *"the grounds for confidence that the set of intended cybersecurity and data privacy controls in a system, application or service are effective in their application."*[14] Since assurance is relative to a specific set of controls, defects in those controls affect the underlying confidence in the ability of those controls to operate as intended to produce the stated results.

Assurance helps define:

- The level of confidence that a stakeholder has that an objective is achieved, that takes into consideration the risks associated with non-conformity (e.g., non-compliance).
- The anticipated, necessary cost to demonstrate conformity with the specified controls.

Risk assessment levels are based on assessment rigor (assurance level). There are three (3) levels of rigor that an organization can select for risk assessments, based on assessment methods described in NIST SP 800-172A Appendix C.[15] There are three (3) levels of rigor:

1. Standard;
2. Enhanced; and
3. Comprehensive

Risk assessment rigor pertains to how risk is assessed. The three (3) assessment methods are:

1. Examining,
2. Interviewing; and
3. Testing

The definition of each assessment method includes types of objects to which the method can be applied. In addition, the application of each method is described in terms of the attributes of depth and coverage.

- The depth attribute addresses the rigor and level of detail of the assessment.
- The coverage attribute addresses the scope or breadth of the assessment.

LEVEL 1 RIGOR: STANDARD

Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are:

1. Implemented; and
2. Free of obvious errors.

Standard rigor represents sufficient due care in the evaluation of cybersecurity and/or data protection controls. Standard rigor is appropriate for the Manual Point In Time (MPIT) assessment methodology that:

1. Is relevant to a specific point in time (time at which the controls were evaluated); and
2. Relies on the manual review of artifacts to derive a finding.

STANDARD Assessment Rigor	EXAMINE	INTERVIEW	TEST
Assessment Method	The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or	The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.

[14] *NIST Glossary - https://csrc.nist.gov/glossary/term/assurance*
[15] *NIST SP 800-172A - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172A.pdf*

		obtain evidence.		
Assessment Results		Results from examination, interviews and testing are used to support the determination of: ▪ Security safeguard existence; ▪ Functionality; ▪ Correctness; ▪ Completeness; and ▪ Potential for improvement over time. Standard rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether the applicable controls are: 1. Implemented; and 2. Free of obvious errors.		
Attributes	Assessment Depth	An examination that consists of high-level reviews, checks, observations or inspections of the assessment object. This type of examination is conducted using a limited body of evidence or documentation including: ▪ Functional-level descriptions for mechanisms; ▪ High-level process descriptions for activities; and ▪ Documents for specifications.	An interview that consists of broad-based, high-level discussions with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions.	A test methodology assumes no knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as "black box" testing. This type of testing is conducted using: ▪ A functional specification for mechanisms; and A high-level process description for activities.
Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.
	Activities	Review procedures associated with:	N/A	Test applicable procedures for:

		▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.		▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	N/A

LEVEL 2 RIGOR: ENHANCED

Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:

1. The applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors; and
2. There are increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended.

Enhanced rigor is appropriate for the Automated Point In Time (APIT) assessment methodology that utilizes automation to augment a traditional assessment methodology, where AAT is used to compare the desired state of conformity versus the current state via machine-readable configurations and/or assessment evidence:

1. Is relevant to a specific point in time (time at which the controls were evaluated);
2. In situations where technology cannot evaluate evidence, evidence is manually reviewed; and
3. The combined output of automated and manual reviews of artifacts is used to derive a finding.

<table>
<tr><th colspan="2">ENHANCED
Assessment Rigor</th><th>EXAMINE</th><th>INTERVIEW</th><th>TEST</th></tr>
<tr><td colspan="2">Assessment Method</td><td>The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.</td><td>The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.</td><td>The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.</td></tr>
<tr><td colspan="2">Assessment Results</td><td colspan="3">Results from examination, interviews and testing are used to support the determination of:
▪ Security safeguard existence;
▪ Functionality;
▪ Correctness;
▪ Completeness; and
▪ Potential for improvement over time.

Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:
1. The applicable controls are:
a. Implemented; and
b. Free of obvious/apparent errors; and
2. There are increased grounds for confidence that the applicable controls are:
a. Implemented correctly; and
b. Operating as intended.</td></tr>
<tr><td rowspan="2">Attributes</td><td>Assessment Depth</td><td>An examination that consists of high-level reviews, checks, observations or inspections and more in-depth studies and analyses of the assessment object. This type of examination is conducted using a substantial body of</td><td>An interview that consists of broad-based, high-level discussions and more in-depth discussions in specific areas with individuals or groups of individuals.

This type of interview is conducted using:</td><td>A test methodology assumes some knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as “gray box” testing.

This type of testing is</td></tr>
</table>

		evidence or documentation. Examples include: ▪ Functional-level descriptions and where appropriate and available, high-level design information for mechanisms; ▪ High-level process descriptions and implementation procedures for activities; and ▪ Documents and related documents for specifications.	▪ A set of generalized, high-level questions; and ▪ More in-depth questions in specific areas where responses indicate a need for more in-depth investigation.	conducted using: ▪ A functional specification and limited system architectural information (e.g., high-level design) for mechanisms and a high-level process description; and ▪ A high-level description of integration into the operational environment for activities.
Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities:	N/A

			▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	

LEVEL 3 RIGOR: COMPREHENSIVE

Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:

1. Whether the applicable controls are:
    a. Implemented; and
    b. Free of obvious/apparent errors;
2. Whether there are further increased grounds for confidence that the applicable controls are:
    a. Implemented correctly; and
    b. Operating as intended on an ongoing and consistent basis; and
3. There is support for continuous improvement in the effectiveness of the applicable controls.

Comprehensive rigor is appropriate for the Automated Evidence with Human Review (AEHR) assessment methodology that is used for ongoing, continuous control assessments:

1. AAT continuously evaluates controls by comparing the desired state of conformity versus the current state through machine-readable configurations and/or assessment evidence; and
2. Recurring human reviews:
    a. Evaluate the legitimacy of the results from automated control assessments; and
    b. Validate the automated evidence review process to derive a finding.

COMPREHENSIVE Assessment Rigor	EXAMINE	INTERVIEW	TEST
Assessment Method	The process of checking, inspecting, reviewing, observing, studying or analyzing one or more assessment objects to facilitate understanding, achieve clarification or obtain evidence.	The process of conducting discussions with individuals or groups in an organization to facilitate understanding, achieve clarification or lead to the location of evidence.	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior.
Assessment Results	Results from examination, interviews and testing are used to support the determination of: ▪ Security safeguard existence; ▪ Functionality; ▪ Correctness; ▪ Completeness; and ▪ Potential for improvement over time. Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining: 1. Whether the applicable controls are: a. Implemented; and b. Free of obvious/apparent errors; 2. Whether there are further increased grounds for confidence that the applicable controls are: a. Implemented correctly; and b. Operating as intended on an ongoing and consistent basis; and 3. There is support for continuous improvement in the effectiveness of the applicable controls.		

Attributes	Assessment Depth	An examination that consists of high-level reviews, checks, observations or inspections and more in-depth, detailed and thorough studies and analyses of the assessment object.
		
		This type of examination is conducted using an extensive body of evidence or documentation including:
		▪ Functional-level descriptions and where appropriate and available:
		  ○ High- level design information;
		  ○ Low-level design information; and
		  ○ Implementation information for mechanisms;
		▪ High-level process descriptions and detailed implementation procedures for activities; and
		▪ Documents and related documents for specifications.
			An interview that consists of broad-based, high-level discussions and more in-depth, probing discussions in specific areas with individuals or groups of individuals.
			
			This type of interview is conducted using:
			▪ A set of generalized, high-level questions; and
			▪ More in-depth, probing questions in specific areas where responses indicate a need for more in-depth investigation.
				Test methodology that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. This methodology is also referred to as "white box" testing.
				
				This type of testing is conducted using:
				▪ A functional specification;
				▪ Extensive system architectural information (e.g., high-level design, low-level design);
				▪ Implementation representation (e.g., source code, schematics) for mechanisms;
				▪ A high-level process description; and
				▪ A detailed description of integration into the operational environment for activities.

	Breadth of Coverage	Examinations uses a sufficiently large sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage
		necessary for determining:
		▪ Whether the applicable controls are:
		  ○ Implemented; and
		  ○ Free of obvious/apparent errors;
		▪ Whether there are further increased grounds for confidence that the applicable controls are:
			Interviews use a sufficiently large sample of individuals in organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining:
			▪ Whether the applicable controls are:
			  ○ Implemented; and
			  ○ Free of obvious/apparent errors;
			▪ Whether there are further increased grounds for confidence that the applicable controls are:
			  ○ Implemented correctly; and
				Testing uses a sufficiently large sample of assessment objects by type and number within type and other specific assessment objects deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining:
				▪ Whether the applicable controls are:
				  ○ Implemented; and
				  ○ Free of obvious/apparent errors;
				▪ Whether there are further increased grounds for confidence that the applicable controls are:
				  ○ Implemented correctly; and

		○ Implemented correctly; and ○ Operating as intended on an ongoing and consistent basis; and ▪ There is support for continuous improvement in the effectiveness of the applicable controls.	○ Operating as intended on an ongoing and consistent basis; and ▪ There is support for continuous improvement in the effectiveness of the applicable controls.	○ Operating as intended on an ongoing and consistent basis; and ▪ There is support for continuous improvement in the effectiveness of the applicable controls.
Assessment Objects	Specifications	Review: ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs.	N/A	N/A
	Mechanisms	Review configurations and/or functionality implemented in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.	N/A	Test functionality in: ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware.
	Activities	Review procedures associated with: ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises.	N/A	Test applicable procedures for: ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.).
	Individuals or Groups	N/A	Conduct interviews with applicable stakeholders associated with control execution and/or oversight. Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities: ▪ Responsible - People directly responsible for performing a task (e.g., control/process operator); ▪ Accountable - Person overall responsible for the task being performed and has the authority to delegate	N/A

			the task to others (e.g., control/process owner); ▪ Supportive - People under the coordination of the Responsible person for support in performing the task; ▪ Consulted - People not directly involved in task execution but were consulted for subject matter expertise; and ▪ Informed - People not involved in task execution but are informed when the task is completed.	

APPENDIX C: NIST SP 800-171 & CMMC RISK MANAGEMENT CONSIDERATIONS

An immediate need for many organizations is compliance with NIST SP 800-171 R2 and the Cybersecurity Maturity Model Certification (CMMC) 2.0. The Cybersecurity & Data Privacy Risk Management Model (C|P-RMM) is a tool that can be used to address the following requirements:

NIST SP 800-171 CONTROLS

These NIST SP 800-171 controls are directly impacted by the C|P-RMM:

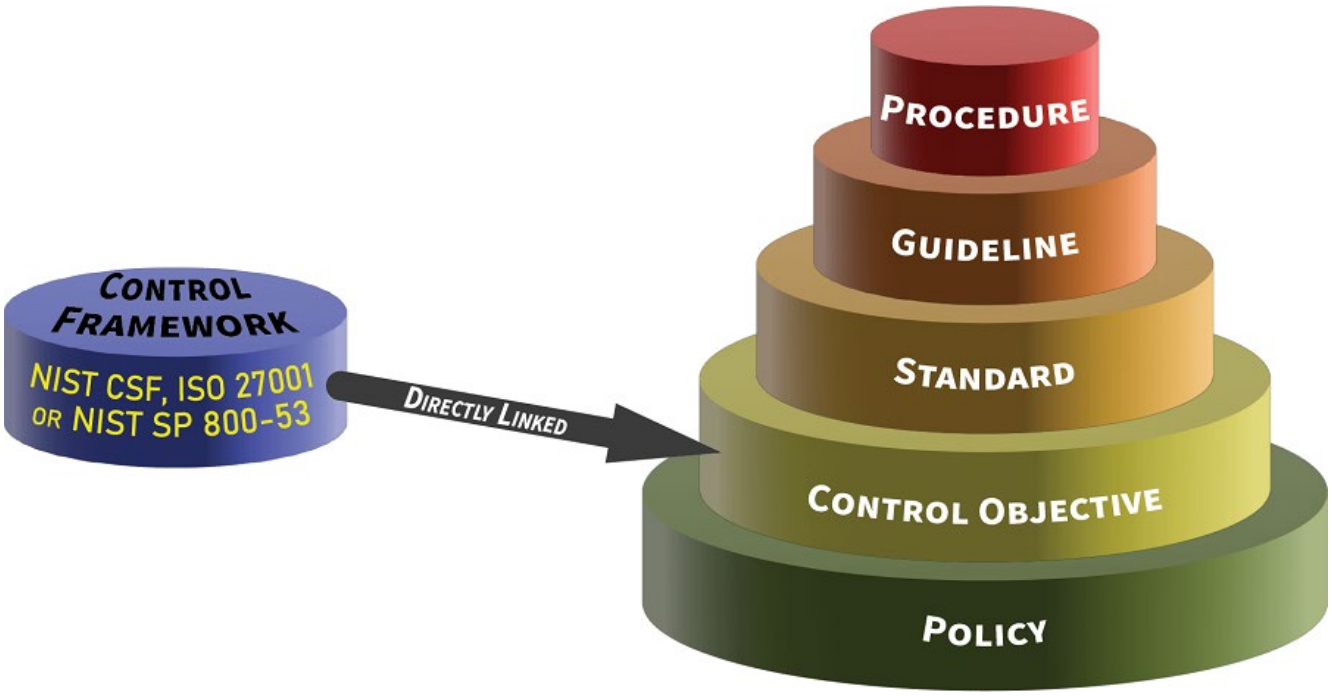
- 3.11.1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
- 3.11.2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
- 3.11.3. Remediate vulnerabilities in accordance with risk assessments.
- 3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
- 3.12.2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
- 3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

APPENDIX D: DOCUMENTATION TO SUPPORT RISK MANAGEMENT PRACTICES

In the context of good cybersecurity documentation, components are hierarchical and build on each other to build a strong governance structure that utilizes an integrated approach to managing requirements. Well-designed documentation is generally comprised of six (6) main parts:

1. Policies establish management's intent;
2. Control Objectives identify leading practices (mapped to requirements from laws, regulations and frameworks);
3. Standards provide quantifiable requirements;
4. Controls identify desired conditions that are expected to be met (requirements from laws, regulations and frameworks);
5. Procedures / Control Activities establish how tasks are performed to meet the requirements established in standards and to meet controls; and
6. Guidelines are recommended, but not mandatory.

Documentation works best when it is simple and concise. Conversely, documentation fails when it is overly wordy, complex or difficult for users to find the information they are seeking. When you picture this from a hierarchical perspective, everything builds off of the policy and all of the components of cybersecurity documentation build off each other to make a cohesive approach to addressing a requirement:

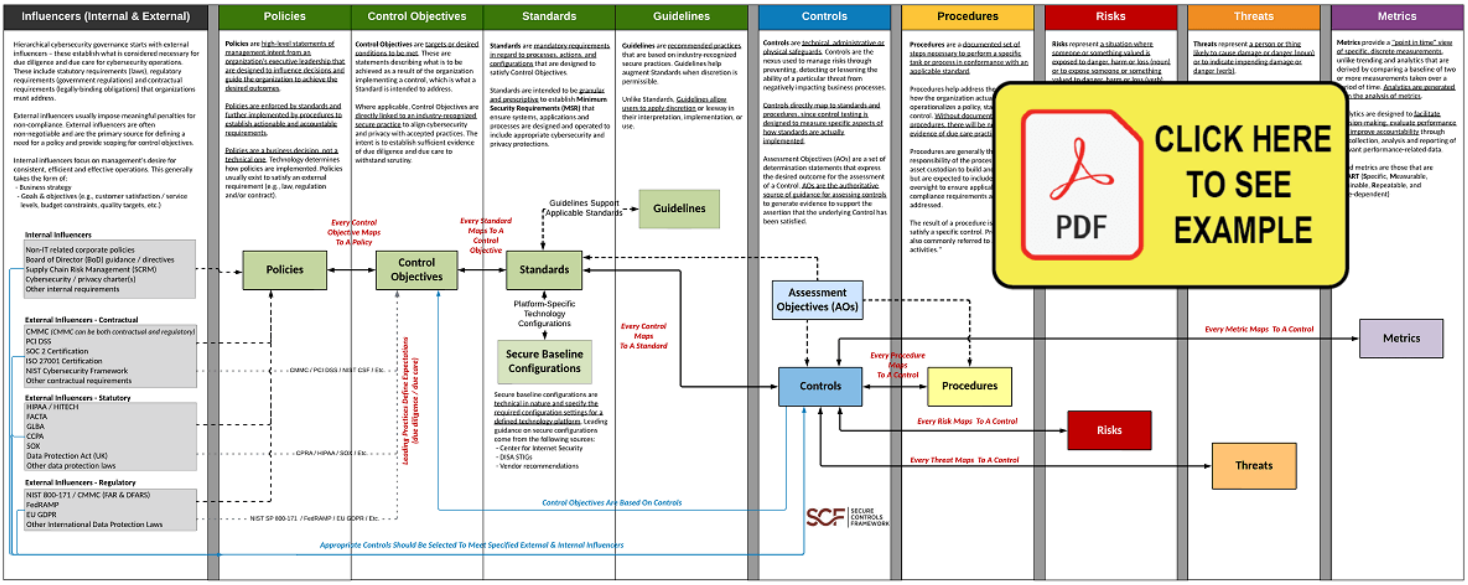


SUPPORTING POLICIES, STANDARDS & PROCEDURES

The purpose of a company's cybersecurity & data privacy documentation is to prescribe a comprehensive framework for:

- Creating a clearly articulated approach to how your company handles cybersecurity & data privacy.
- Protecting the confidentiality, integrity, availability and safety of data and systems on your network.
- Providing guidance to help ensure the effectiveness of cybersecurity and data privacy controls that are put in place to support your company's operations.
- Helping your users to recognize the highly-networked nature of the current computing environment to provide effective company-wide management and oversight of those related cybersecurity and data privacy risks.

When that is all laid out properly, your company's cybersecurity and data privacy documentation should flow like the diagram below depicts, where your organization's cybersecurity and data privacy policies are linked all the way down to metrics: https://complianceforge.com/content/pdf/complianceforge-hierarchical-cybersecurity-governance-framework.pdf



RISK MANAGEMENT PROGRAM (RMP)

ComplianceForge developed its Risk Management Program (RMP) as a way to document risk management practices at the strategic, operational and tactical levels. All organizations have a need to manage risk. Most organizations are compelled to manage risk and these requirements come from a broad range of statutory, regulatory and contractual origins. Regardless of your industry, requirements to manage cybersecurity risk exist and failing to manage risk could leave your organization exposed to liabilities from non-compliance:

- NIST SP 800-171 & CMMC. Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations – Multiple sections of NIST SP 800-171 & CMMC requires risk to be periodically.
- Federal Trade Commission (FTC) Act. 15 U.S. Code § 45 deems unfair or deceptive acts or practices in or affecting commerce to be unlawful - poor security practices are covered under this requirement and not managing cybersecurity risk is an indication of poor security practices.
- Payment Card Industry Data Security Standard (PCI DSS). Section 12.2 requires companies to perform a formal risk assessment.
- Health Insurance Portability and Accountability Act (HIPAA). Security Rule (Section 45 C.F.R. §§ 164.302 – 318) requires companies to conduct an accurate & thorough assessment of potential risks.
- Gramm-Leach-Bliley Act (GLBA). Safeguard Rule requires companies to identify and assess risks to customer information.
- Massachusetts MA 201 CMR 17.00. Section 17.03(2)(b) requires companies to "identify & assess" reasonably-foreseeable internal and external risks.
- Oregon Identity Theft Protection Act. Section 646A.622(2)(d)(B)(ii) requires companies to assess risks in information processing, transmission & storage.
- Vendor Contracts. It is increasingly common for vendors, partners and subcontractors to be contractually-bound to perform recurring risk assessments. Not having a risk management program could lead to breach of contract or losing a bid.