



**COMPLIANCE
FORGE**

Enterprise Risk Management (ERM)

Practitioner's Guide To Align Risk Appetite, Risk Tolerance & Risk Thresholds With Strategic, Operational & Tactical Business Planning Activities

version 2024.2

Copyright © 2024. Compliance Forge, LLC (ComplianceForge). All rights reserved.

Disclaimer: This document is provided for educational purposes only. This document does not render professional services and is not a substitute for professional services. If you have compliance questions, you are encouraged to consult a competent cybersecurity and/or data privacy professional.

TABLE OF CONTENTS

| | |
|---|-----------|
| Executive Summary | 4 |
| Introduction | 5 |
| Summarizing The Integration Of Risk Management & Business Planning | 6 |
| Risk Management: Strategic Considerations | 7 |
| <i>Mission</i> | 7 |
| <i>Vision</i> | 7 |
| <i>Strategy</i> | 7 |
| <i>Compliance Obligations</i> | 7 |
| <i>Risk Appetite</i> | 7 |
| Risk Management: Operational Considerations | 7 |
| <i>Line of Business (LOB) Objectives</i> | 7 |
| <i>Capability Maturity Targets</i> | 7 |
| <i>Resource Prioritization</i> | 7 |
| <i>Risk Tolerance</i> | 7 |
| Risk Management: Tactical Considerations | 8 |
| <i>Department / Team Objectives</i> | 8 |
| <i>Processes</i> | 8 |
| <i>Technologies</i> | 8 |
| <i>Staffing</i> | 8 |
| <i>Supply Chain</i> | 8 |
| <i>Risk Thresholds</i> | 8 |
| <i>Operational Risk</i> | 8 |
| Baselining Risk Management Terminology | 9 |
| Understanding The Differences Between: Risks vs Threats | 10 |
| <i>What Is A Risk?</i> | 10 |
| <i>What Is A Threat?</i> | 13 |
| Understanding The Differences Between: Risk Tolerance vs Risk Threshold vs Risk Appetite | 13 |
| <i>What Is A Risk Appetite?</i> | 13 |
| <i>What Is A Risk Tolerance?</i> | 13 |
| <i>What Is A Risk Threshold?</i> | 16 |
| Practical Risk Management Example | 16 |
| Baselining Business Planning Terminology | 18 |
| The Hierarchical Nature of Vision, Mission, Strategy & Objectives | 18 |
| Understanding The Differences Between: Mission vs Vision vs Strategy | 19 |
| <i>What Is a Mission Statement?</i> | 19 |
| <i>What Is A Vision Statement?</i> | 20 |
| <i>What Is A Strategy?</i> | 21 |
| <i>What Are Objectives?</i> | 22 |
| <i>What Are Operations?</i> | 22 |
| <i>What Are Tactics?</i> | 22 |
| Business Planning Considerations: Avoiding Negligence | 22 |
| <i>Defining Negligence As It Pertains To Cybersecurity & Data Privacy</i> | 23 |
| <i>Determining A Breach Of Duty</i> | 24 |
| <i>Determining Whether There Was A Duty To Act</i> | 24 |
| Applying The Concepts Of Assurance, Conformity & Materiality To Risk Management | 25 |
| Assurance Levels: Defining Criteria For Rigor In Assessing Risk | 25 |
| <i>Level 1 Rigor: STANDARD</i> | 25 |
| <i>Level 2 Rigor: ENHANCED</i> | 25 |
| <i>Level 3 Rigor: COMPREHENSIVE</i> | 25 |
| Conformity: Defining A Risk Determination | 26 |
| <i>Risk Determination: STRICTLY CONFORMS</i> | 26 |
| <i>Risk Determination: CONFORMS</i> | 26 |
| <i>Risk Determination: SIGNIFICANT DEFICIENCY</i> | 27 |
| <i>Risk Determination: MATERIAL WEAKNESS</i> | 27 |
| Materiality: Criteria To Establish Risk Thresholds | 29 |
| Historical Context For Cybersecurity & Data Privacy Materiality Usage | 29 |
| Common Materiality Thresholds | 29 |
| Material Weakness vs Material Control vs Material Risk vs Material Threat vs Material Incident | 31 |
| <i>Material Weakness</i> | 31 |
| <i>Material Control</i> | 31 |
| <i>Material Risk</i> | 31 |
| <i>Material Threat</i> | 32 |
| <i>Material Incident</i> | 32 |

Security & Exchange Commission (SEC) – Cybersecurity Risk Management, Strategy, Governance & Incident

| | |
|--|-----------|
| Disclosure | 33 |
| Defining Risk Management & Governance Practices | 33 |
| 17 CFR 229.106(b) - Risk Management & Strategy | 33 |
| 17 CFR 229.106(c) - Governance | 33 |
| Public Disclosure Requirement For Cybersecurity Incidents | 33 |
| Form 8-K Item 1.05 – Material Cybersecurity Incidents | 33 |
| Referenced Frameworks & Supporting Practices | 35 |
| Appendices | 36 |
| Appendix A: Assessment Rigor | 36 |
| Level 1 Rigor: Standard | 36 |
| Level 2 Rigor: Enhanced..... | 39 |
| Level 3 Rigor: Comprehensive | 42 |

EXECUTIVE SUMMARY

The alternative to risk management is crisis management. This document provides practical guidance on risk management for cybersecurity and data privacy practitioners, specifically focused on how to align risk appetite, risk tolerance and risk thresholds with an organization's strategic, operational and tactical business planning activities. What is presented is an integrated approach that has practical applications.

If you take the time to read this document, we are confident that your understanding of this topic will be greatly enhanced. The concepts of risk appetite, risk tolerance and risk thresholds are not independent terms that are meant to stand by themselves, since they share a dependency that needs to be understood to create a coherent risk management strategy. Likewise, those terms are also directly linked to strategic, operational and tactical decision making.

Organizations invest in cybersecurity and data privacy as a necessity. This necessity is driven in large part by statutory, regulatory and contractual requirements. It is also driven by the desire to protect the organization's brand from acts that would harm its public image. Regardless of the reason, the base expectation is that those charged with developing, implementing and governing the cybersecurity and data privacy functions are doing so in a reasonable manner that would withstand scrutiny that could take the form as an external auditor, regulator or prosecuting attorney.

The intent of this document is to prove how integrating business planning with risk management practices is in your organization's best interest, since it can decrease liability and increase the effectiveness those cybersecurity and data privacy practitioners who are working to implement the organization's strategy. Key takeaways are:

- **Take Away #1:** Risk management is not meant to be “bolted on” as an afterthought. Criteria to define and manage risk need to be integrated into the development of mission, vision and strategy statements, since those decisions (or indecisions) directly affect operational objectives, which flows down to the work of individual contributors at the team and department levels.
- **Take Away #2:** How risk is defined needs to be standardized across the organization. A risk designation (e.g., Moderate Risk or High Risk) must share a common definition of financial and/or operational impact across cybersecurity / IT, legal, finance, HR, operations, etc. Standardization enables an “apples to apples” comparison that can aid in creating a more holistic approach to risk management practices when risk designations mean the same thing across the organization.
- **Take Away #3:** Risks and threats are variable - they change and are not static. The implication is that risk ratings and threat assessments are subject to change as the operating environment changes. Logically, this means risk management decisions should not be “written in stone” and must be re-evaluated in a similar context to how recurring business planning practices exist that convene stakeholders to generate updated business plans, as necessary. This infers that the risk appetite, risk tolerance and risk thresholds are meant to be flexible enough to adapt to changing business circumstances that affect an organization's industry, including evolving compliance obligations.
- **Take Away #4:** Goals are not a strategy. This document covers the terminology associated with business planning, so that you have a solid basis to work from, since terminology associated with mission, vision, strategy, etc. are often misused. Business planning activities have a direct impact on risk management practices.
- **Take Away #5:** Understanding the concept of negligence is important in the context of business planning and risk management, since your organization's business plan is evidence of due diligence and due care in addressing applicable compliance obligations. Business planning is all about identifying appropriate practices that need to be implemented, generally in a risk-prioritized manner that might span an execution timeline over several years.
- **Take Away #6:** An indicator of a well-run cybersecurity and data privacy program is where staff at all levels clearly know their role in making the organization successful because the leadership implemented a vision, mission and strategy to drive its operations to achieve its stated goals.



Tom Cornelius

Senior Partner, ComplianceForge
Founder, Secure Controls Framework (SCF)



Andy Kuykendall

Board of Advisors, Secure Controls Framework (SCF) Council

INTRODUCTION

Organizations often face conflicting expectations for risk management, based on department-level practices. 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.

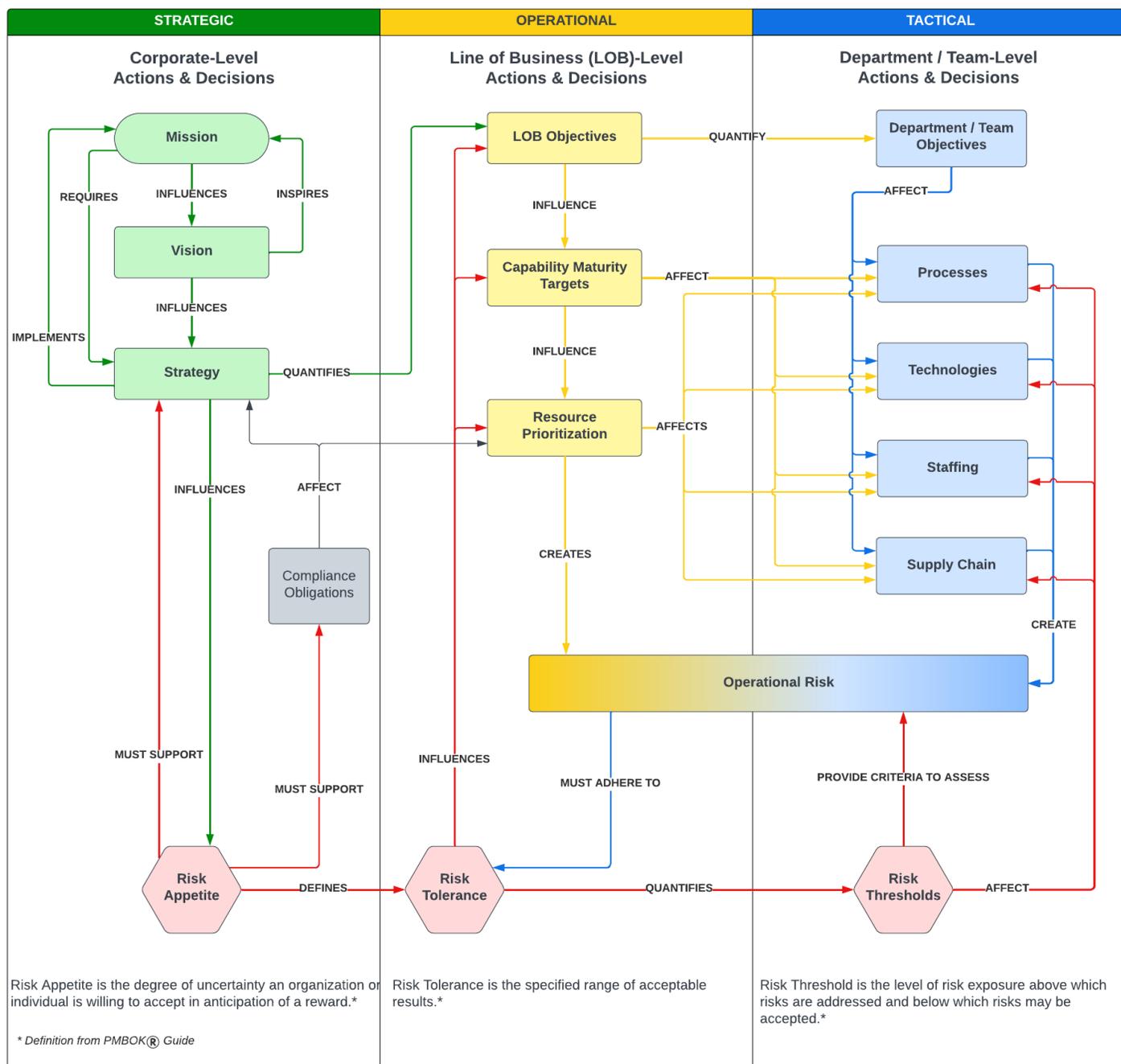
What is important to keep at the forefront of risk management considerations is the material nature of risk, as it pertains to the organization. Risks that have a material impact include, but are not limited to:

- 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.).

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:

- 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.



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 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, 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

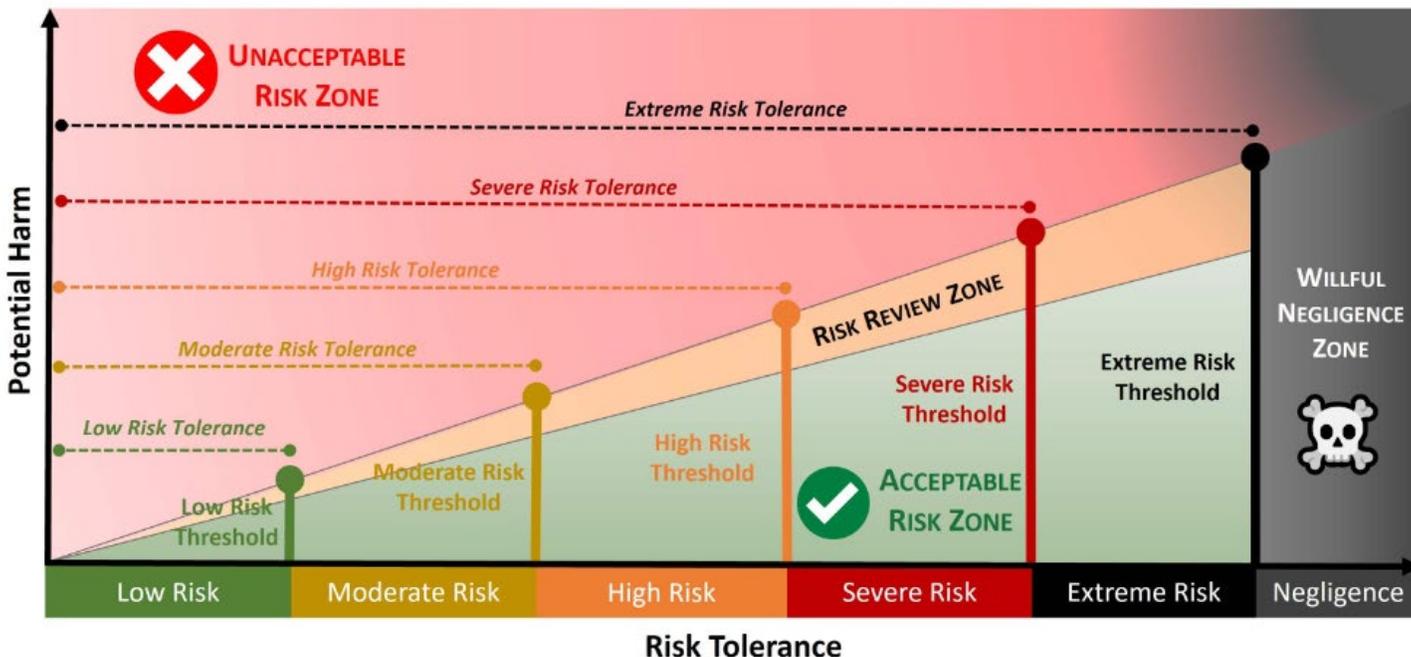
- Is assessed against the organization's risk thresholds.
- Must adhere to the organization's risk tolerance, where the organization has four (4) options to address identified risks:
 1. Reduce the risk to an acceptable level;
 2. Avoid the risk;
 3. Transfer the risk to another party; or
 4. Accept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

BASELINING RISK MANAGEMENT TERMINOLOGY

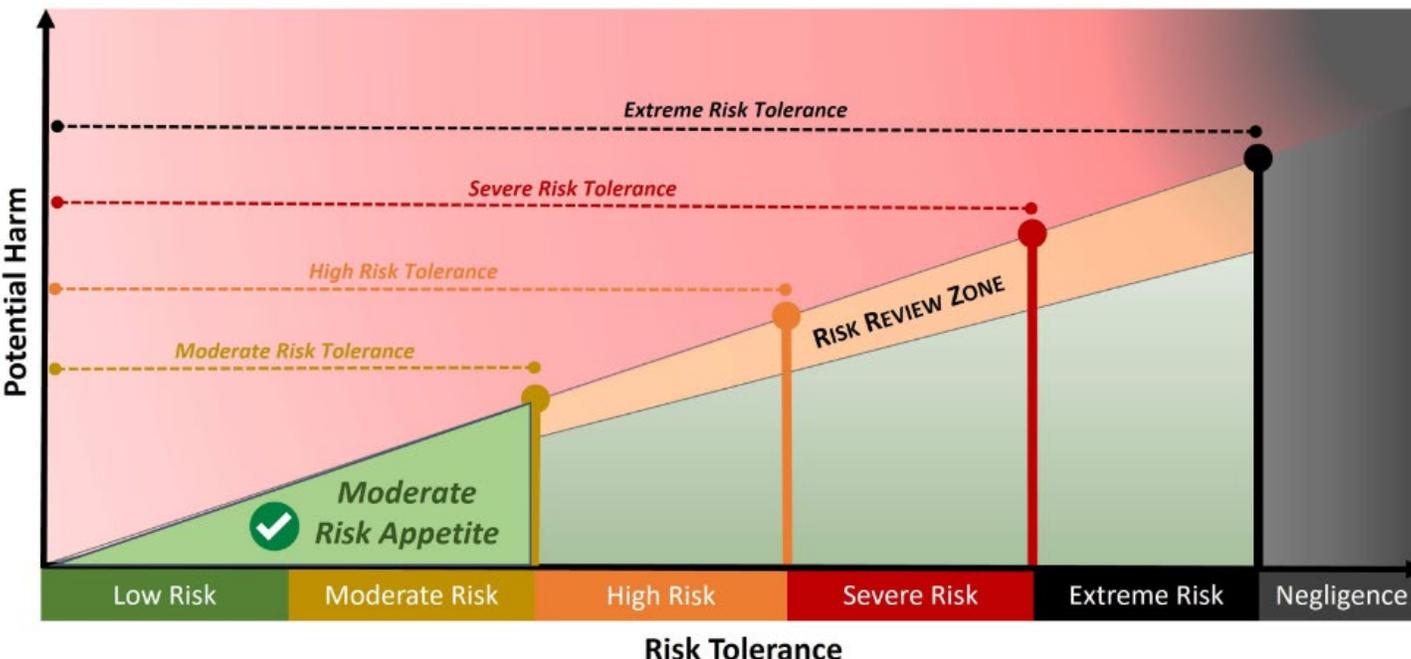
Risk management involves coordinated activities that optimize the management of potential opportunities and adverse effects. Proactive risk management activities provide a way to realize potential opportunities without exposing an organization to unnecessary peril.

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:

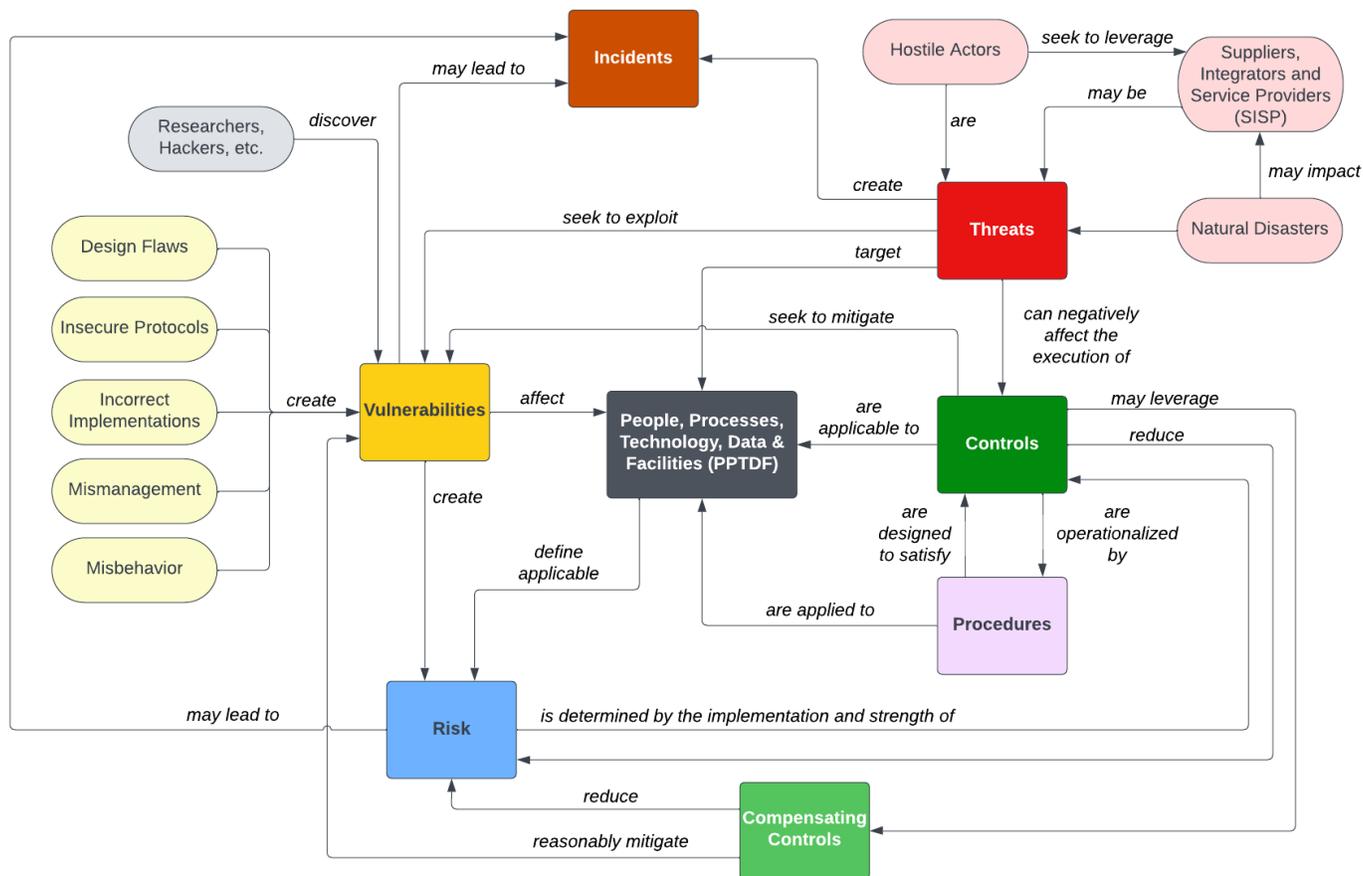


UNDERSTANDING THE DIFFERENCES BETWEEN: RISKS VS THREATS

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



WHAT IS A RISK?

In the context of risk management 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.*

RISK MANAGEMENT OPTIONS

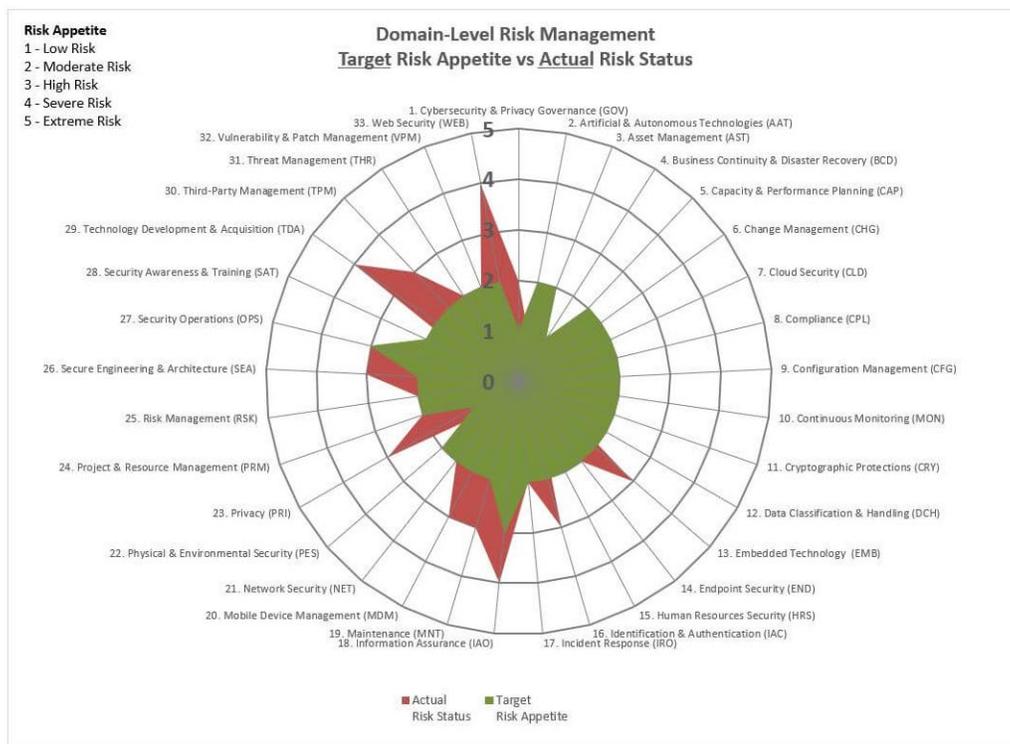
Traditional risk management practices have four (4) options to address identified risk:

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

¹ Risk vs Threat vs Vulnerability Ecosystem - <https://complianceforge.com/content/Risk-vs-Threat-vs-Vulnerability.pdf>

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.

To provide greater flexibility, as well as enhanced situational awareness of risk management practices, it is possible to identify a target risk appetite at a domain-level, rather than a single risk appetite at an organizational-level. Using a review of current risk status vs target risk appetites can be useful to see how well cybersecurity practices operate to clearly see what practice areas deviate from expectations - this can be visualized with a spider / radar diagram, as shown below that applies a risk appetite to each of the thirty-three (33) Secure Controls Framework (SCF) domains.



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

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).² The C|P-RMM:

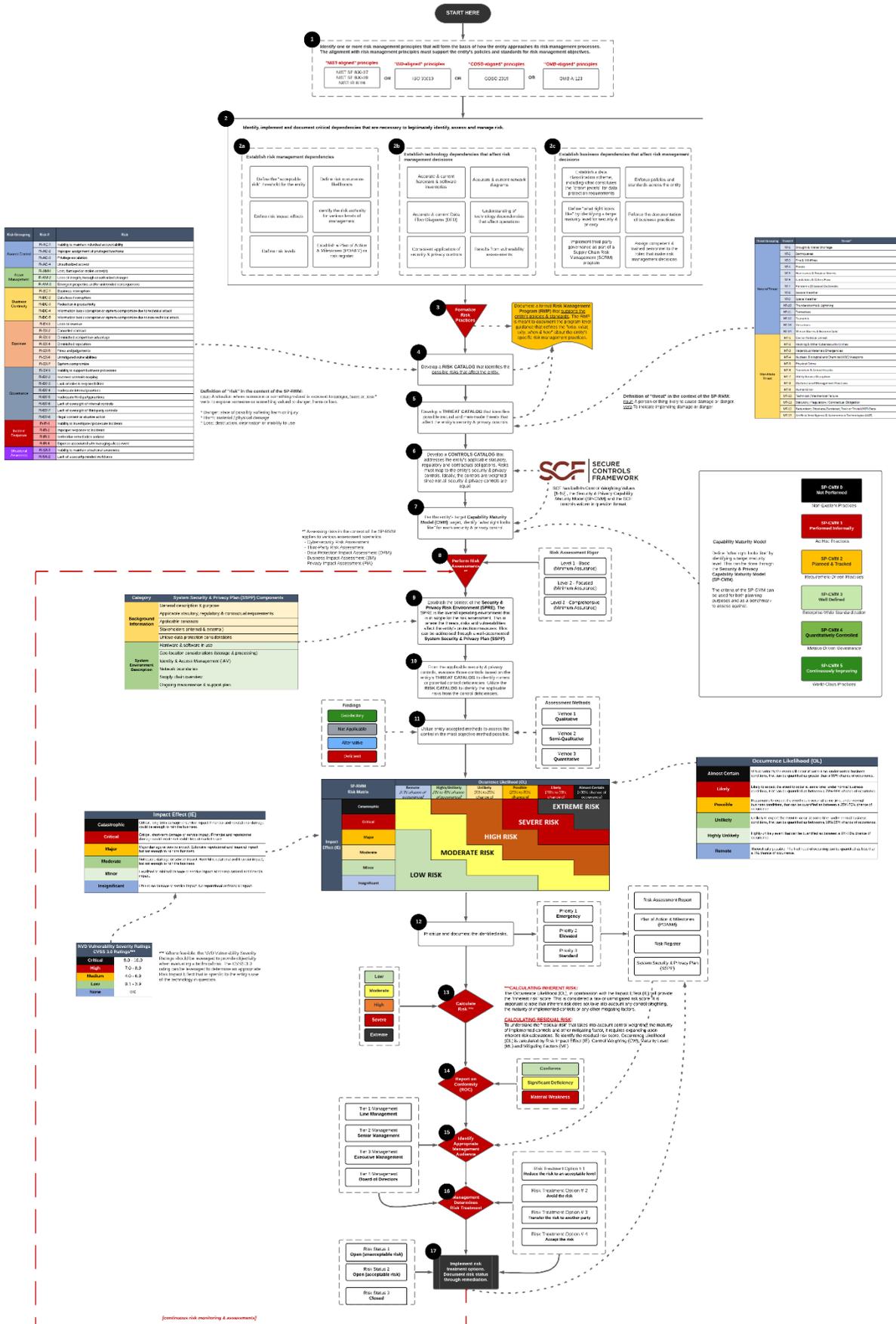
- Is a free solution that organizations can use to holistically approach that breaks risk management down into seventeen (17) distinctive steps;
- Exists is to help cybersecurity and data privacy functions create a repeatable methodology to identify, assess, report and mitigate risk;
- Offers flexibility 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).

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 of the following risk determinations:

- Conforms;
- Significant Deficiency; or
- Material Weakness

² SCF Cybersecurity & Data Privacy Risk Management Model (C|P-RMM) - <https://securecontrolsframework.com/risk-management-model/>

Security & Privacy Risk Management Model (SP-RMM)



WHAT IS A THREAT?

In the context of risk management 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

According to the Project Management Body of Knowledge (PMBOK®) Guide:³

- **Risk Appetite:** *the degree of uncertainty an organization or individual is willing to accept in anticipation of a reward.*
- **Risk Tolerance:** *the specified range of acceptable results.*
- **Risk Threshold:** *the level of risk exposure above which risks are addressed and below which risks may be accepted.*

WHAT IS A RISK APPETITE?

A risk appetite is the collective amount of risk that an organization is willing to take and is usually agreed upon by senior members of management.

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.⁴

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.

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 and quantify the impact of a risk, enabling risk assessments to leverage that same criteria, as well as 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.

³ PMBOK® Guide - <https://www.pmi.org/pmbok-guide-standards/foundational/pmbok>

⁴ ComplianceForge Hierarchical Cybersecurity Governance Framework (HCGF) - <https://complianceforge.com/content/Hierarchical-Cybersecurity-Governance-Framework.pdf>

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**).

| SP-RMM Risk Matrix | | Occurrence Likelihood (OL) | | | | | |
|--------------------|---------------|--------------------------------------|---|---|---|---|---|
| | | Remote [<1% chance of occurrence] | Highly Unlikely [1% to 10% chance of occurrence] | Unlikely [10% to 25% chance of occurrence] | Possible [25% to 70% chance of occurrence] | Likely [70% to 99% chance of occurrence] | Almost Certain [>99% chance of occurrence] |
| Impact Effect (IE) | Catastrophic | | | | | | EXTREME RISK |
| | Critical | | | | | | SEVERE RISK |
| | Major | | | | | | HIGH RISK |
| | Moderate | | | | | | MODERATE RISK |
| | Minor | | | | | | LOW RISK |
| | Insignificant | | | | | | LOW RISK |

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 Severe 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 an Extreme Risk Tolerance include, but are not limited to:

- Startups
- 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., Low, Moderate and High Risk). By establishing these risk thresholds, it provides a means of comparing relative risk to an organization. Risk thresholds are criteria that are unique to an organization such as organization-specific activities / scenarios that could:

- Damage the organization's reputation;
- Negatively affect short-term and long-term profitability; and/or
- 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.

PRACTICAL RISK MANAGEMENT EXAMPLE

For an example scenario, a theoretical company is experimenting with 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)?

These are all very real topics that need to be considered and how risk is managed has significant legal and financial implications.

BASELINING BUSINESS PLANNING TERMINOLOGY

It is important to level-set on a few fundamental business planning components - strategy, operations and tactics. While these terms are used by organizations across the globe, the terms have their origins in military planning where the terms have specific scopes that are important to understand. Hierarchically, tactics support operations and operations support strategy.

STRATEGY > OPERATIONS > TACTICS

The discussion of “strategy vs operations vs tactics” primarily comes down to the concept of defining doctrine. The concepts of strategy, operations and tactics are directly rooted in military planning. The US Army’s formalization of this specific doctrine occurred in the 1982 release of **Field Manual (FM) 100-5** as a way to formalize a logical approach to describe the “levels of war” that span from the generals in charge, all the way to the lowly private in the trenches.

In a real-world scenario to gain context, a relevant historical event is *Operation Overlord*, the Allied invasion of Normandy during the Second World War (WW2):

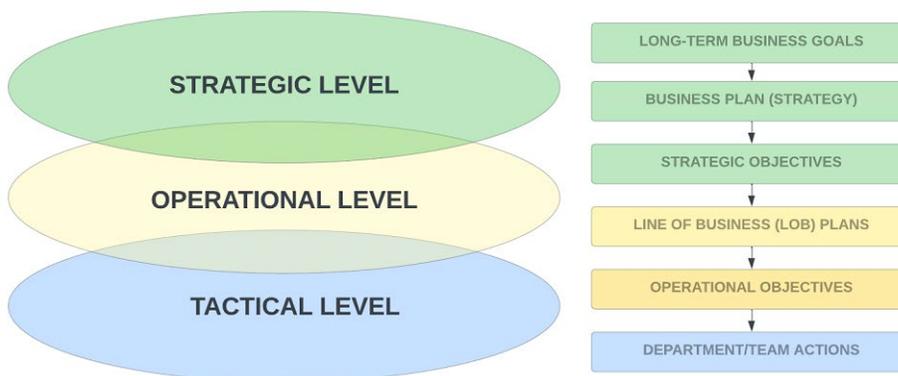
- **Strategy.** The Allies’ high-level plan in Europe was to wage a multi-pronged effort to pressure the Axis powers into an unconditional surrender. This involved the coordination of several heads of state and their military commanders to agree upon a combined approach to win WW2.
- **Operations.** One of these multi-pronged efforts of the Allied strategy involved opening a new front in western Europe by landing Allied forces in France. The D-Day landings as part of *Operation Overlord* were the effort to invade France via multiple beach landings throughout Normandy in June 1944. This involved the coordination of multiple divisions, branches of the military and nations to deliver the appropriate personnel, equipment and supplies at the right time and locations.
- **Tactics.** The actions taken by individual Soldiers and small units were designed to support the larger effort of *Operation Overlord*. Each Soldier had a role in his unit and each unit had a role in the beach landings.

THE HIERARCHICAL NATURE OF VISION, MISSION, STRATEGY & OBJECTIVES

There is overlap between strategic, operational and tactical levels, so there is no clear demarcation that can be uniformly applied to all organizations. The actions of individual contributors at the tactical level stack up to support broader operational goals, which in turn are designed to support a strategy that is aligned with the company’s success. As it applies to the private sector:

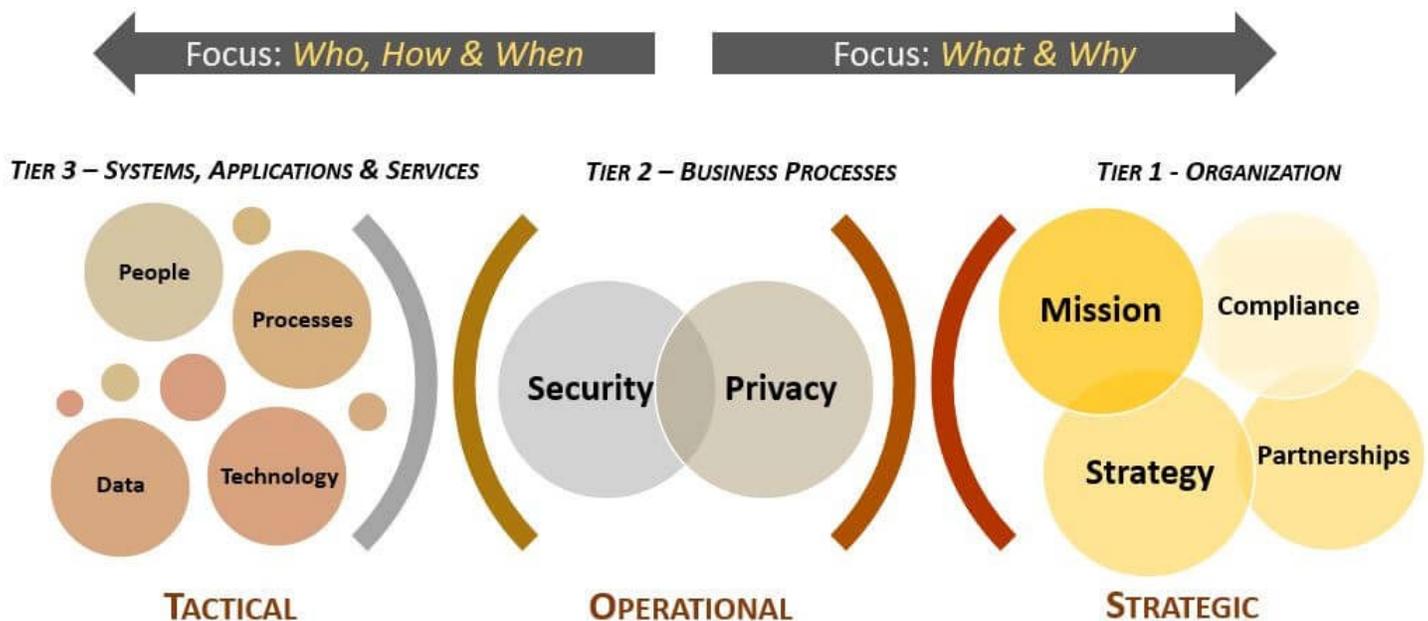
- **Strategic** - At the strategic level, an organization employs available resources to secure its business goals & objectives (e.g., corporate business plan).
- **Operational** - At the operational level, an organization uses available resources to attain those strategic goals & objectives within a specific Line of Business (LOB).
- **Tactical** - At a tactical level, departments/teams employ techniques/procedures to support operational objectives, as defined by the LOB.

The same concept applies to businesses in every industry, since the actions of individual contributors at the tactical level stack up to support broader operational goals, which in turn are designed to support a strategy that is aligned with the company’s success.



In the context of cybersecurity & data privacy considerations, it is possible to overlay the “who, what, when, how & why” across

the strategic, operational and tactical levels as depicted in the graphic below:



UNDERSTANDING THE DIFFERENCES BETWEEN: MISSION VS VISION VS STRATEGY

An indicator of a well-run cybersecurity and data privacy program is where staff at all levels clearly know their role in making the organization successful because the leadership implemented a vision, mission and strategy to drive its operations. This is leadership in its purest form, since it involves providing appropriate direction and then empowering staff to make the right things happen.

WHAT IS A MISSION STATEMENT?

A mission statement describes why an organization is operating and thus provides a framework by which strategies are formulated. It describes:

- What the organization does (e.g., present capabilities);
- Who all it serves (e.g., stakeholders, clients, etc.); and
- What makes an organization unique (e.g., reason for existence).

Mission statements are similar to vision statements, in that they, too, look at the big picture. However, mission statements are more concrete and action-oriented:

- Mission statements answer the question of why your department exists. These statements are outcome-oriented and determine the **“what”** and **“why”** in a straightforward, concise manner.
- Missions are directive in nature by a higher authority to a lower authority (e.g., CEO or board of directors issues a mission to the CISO/CIO/COO/CPO).
- The results of mission execution determine performance ratings for executive management.

A mission statement differentiates an organization from others by explaining its broad scope of activities, its products, and technologies it uses to achieve its goals and objectives. For instance,

- Microsoft’s mission is “to empower every person and every organization on the planet to achieve more.”
- Wal-Mart’s mission is “to save people money so that they can live better.”

Features of a mission statement:

- It must be feasible and attainable.
- It must be credible so all stakeholders will be able to believe it.
- It must be clear enough so that any action can be taken.
- It should be unique and distinctive to leave an impact in everyone’s mind.
- It should be inspiring for all employees (both management and staff).

After having developed possible statements, you will want to ask of each one:

- Does it describe what an organization will do and why it will do it?
- Is it concise (one sentence)?
- Is it outcome oriented?
- Is it inclusive of the goals and people who may become involved in the organization?

Example mission statements:

- *“To deliver high-quality, innovative cybersecurity services and solutions that reduce risk across [company name].”*
- *“To bring inspiration and innovation to every athlete in the world.”*
- *”To provide customers with superb value; high-quality, relevant technology; customized systems; superior service and support; and products and services that are easy to buy and use.”*
- *“To dedicate ourselves to humanity’s quest for longer, healthier, happier lives through innovation in pharmaceutical, consumer and animal health products.”*
- *“To provide fast food customer food prepared in the same high-quality manner world-wide that is tasty, reasonably-priced & delivered consistently in a low-key decor and friendly atmosphere.”*
- *“To develop & deliver the most innovative products, manage customer experience, deliver quality services that contribute to brand strength, establishes a competitive advantage and enhances profitability, thus providing value to the stakeholders of the bank.”*
- *“To be the company that best understands and satisfies the product, service and self-fulfillment needs of women—globally.”*

WHAT IS A VISION STATEMENT?

A vision statement provides an overarching goal for the organization and should inspire employees to dream and motivate them to take action. Vision statements give employees a reminder about what their organization is attempting to develop. It incorporates a shared understanding about the nature and aim of the organization and utilizes this understanding to direct and guide the organization towards a better purpose.

Vision statements communicate the concept of what ideal conditions look like in a perfect world for the execution of the mission.

- Vision statements are meant to appeal to every staff member and should be easily understood by everyone. Quite simply, if a vision statement must be explained, it is a poorly constructed vision statement.
- This is an executive function performed by the CEO to uplift & inspire across the broader organization.

A vision statement identifies where the organization wants or intends to be in future or where it should be to best meet the needs of the stakeholders. It describes dreams and aspirations for the future. For instance:

- Microsoft’s vision is to “help people and businesses throughout the world realize their full potential.”
- Wal-Mart’s vision is to “build a better world — helping people live better and renew the planet while building thriving, resilient communities.”

The best visions are inspirational, clear, memorable, and concise. An effective vision statement must have following features:

- It must be concise.
- It must be unambiguous.
- It must be clear.
- It must harmonize with the organization’s culture and values.
- Dreams and aspirations must be rational & realistic.

In order to realize the vision, it must be deeply instilled in the organization, being owned and shared by everyone involved in the organization. For vision statement validation purposes:

- Will it draw people to common work?
- Does it give hope for a better future?
- Will it inspire employees to realize their dreams through positive, effective action?
- Does it provide a basis for developing the other aspects of your action planning process?

Example vision statements:

- *“We exist to create an environment where security, collaboration and creativity are seamless. In doing so, we will unlock [company name]’s unmeasurable potential to innovate at the speed of inspiration.”*
- *“Our vision is to be earth’s most customer centric company; to build a place where people can come to find and discover anything they might want to buy online.”*
- *“We intend to provide our customers with the best online shopping experience from beginning to end, with a smart,*

searchable website, easy-to-follow instructions, clear and secure payment methods, and fast, quality delivery.”

- *“The [company name] Company will inspire its employees to be the best they can be. We will engage in sustainable practices and anticipate the needs of our customers. We will maximize returns to the stockholders while still maintaining quality in our products. “*
- *“Our vision is to bring our students into the 21st century through innovation and modern technology. Learning will be enhanced with computer software and educational games that will allow students to proceed at their own rate according to their ability.”*
- *“We will be the premier organization operating locally and internationally that provides the complete range of financial services to all segments under one roof.”*

WHAT IS A STRATEGY?

Strategy statements are high-level actions that are coherently arranged to achieve your mission.

- The CEO establishes the big picture of how the company will accomplish its mission.
- Strategies allow for the development of a thoughtfully constructed course of action and the establishment of realistic objectives.
- Business plans are the in-depth documents to implement a strategy through the detailed definition of objectives, resourcing needs and assigning responsibilities.
- The results of strategy execution determine performance ratings for senior leadership (e.g., CISO/CIO/COO/CPO).

Defining the objective, scope and competitive advantage requires trade-offs, which are fundamental considerations to building a strategy. For example, if a company decides to pursue growth, it must accept that profitability will not be a priority. If it decides to serve institutional clients, it may ignore retail customers.

Now that the “what” and “why” are answered with the mission and vision statements, it’s time to address the “how” with a strategy that defines how to bring the vision and mission statements to reality. That’s where setting goals and objectives come into play with a focus of the importance of making them SMART:

- S – **Specific** (target a specific area for improvement)
- M – **Measurable** (quantify or at least suggest an indicator of progress)
- A – **Actionable** (specifically who will do it)
- R – **Realistic** (state what results can realistically be achieved, based on available resources)
- T – **Time-bound** (specify when the results can be achieved)

Strategic intent:

- Gives a picture about what an organization must get into immediately in order to achieve the company’s vision.
- Motivates the people. It clarifies the vision of the company.
- Helps management to emphasize and concentrate on the priorities.
- Influences people to achieve what at first may seem to be unachievable goals.

There are three (3) basic elements of a strategy statement:

1. The objective defines the ends that the strategy is designed to achieve within a specific time frame.
2. The scope is the domain of the business—the part of the business landscape in which your company will operate.
3. The competitive advantage is the essence of your strategy. It determines what you will do differently or better than the competition to achieve your objective.

Example strategy statements:

- *“[company name] will grow from 10,000 to 17,000 financial advisers by 2024 by offering trusted and convenient face-to-face financial advice to conservative individual investors who delegate their financial decisions, through a national network of one-financial- adviser offices.”*
- *“[company name] will increase market penetration in the North America SOHO segment by 20% through improvements in product usability, partner marketing, and customer relationship management leveraging our long-term relationships with customers and deep awareness of their business needs.”*
- *“We will influence key stakeholders to raise the level of technology and security maturity in [company name] so that compliance requirements are proactively addressed in a ‘business as usual’ manner. The role of IT security will evolve from actively managing control execution to a validation and reporting role.” [CISO-level strategy for a cybersecurity department]*

WHAT ARE OBJECTIVES?

Objectives are the short and mid-range goals that are arranged and prioritized to achieve the strategy.

- Objectives are merely the steppingstones that are needed to achieve success in accomplishing the strategy.
- Objectives can be as simple as a bullet point list that documents components necessary to achieve the strategy.
- While this list of objectives is “owned” by the CEO, the Line of Business (LOB) executives are responsible for achieving these objectives through formulating and executing the plans for how their unique operations are conducted and resources are prioritized.
- A responsibility assignment matrix (also known as RACI / RASCI diagrams) is a great tool to assign stakeholder roles and responsibilities to ensure objectives are proactively managed.

Example objectives:

- *“Develop, implement and manage Continuous Monitoring (CM) capabilities to enable the timely identification and response to potential cybersecurity events.”*
- *“Achieve an ISMS maturity level of CMM 3 by 2023 and CMM 4 by 2026.”*

WHAT ARE OPERATIONS?

Operations are mid-level actions that directly link to strategy and objectives – it clarifies how both will actually be accomplished.

- Operations transform strategy and objectives into actionable projects or initiatives that define the required resources for tactics to successfully execute.
- Operations are “owned” by LOB and are responsible for achieving these objectives in how work is prioritized, resourced and managed.
- Poor execution of operations will prevent or inhibit the successful execution of a strategy.
- The results of operations execution determine performance ratings for LOB-level management (e.g., Vice Presidents, department heads, etc.).

WHAT ARE TACTICS?

Tactics are low-level actions that directly link to operations – it specifies how department-level objectives will be achieved on a day-to-day basis through staff assignments, processes and procedures.

- Tactics bring together the people, processes, technology & data to successfully accomplish tasks to achieve assigned objectives.
- Poor execution of tactics will prevent or inhibit the successful execution of operations.
- Tactics are “owned” by managers and directors, who are responsible for achieving these objectives in how work is prioritized, resourced and managed.
- The results of tactics execution determine performance ratings for individual contributors (e.g., risk analysts, engineers, architects, forensic analysts, etc.).

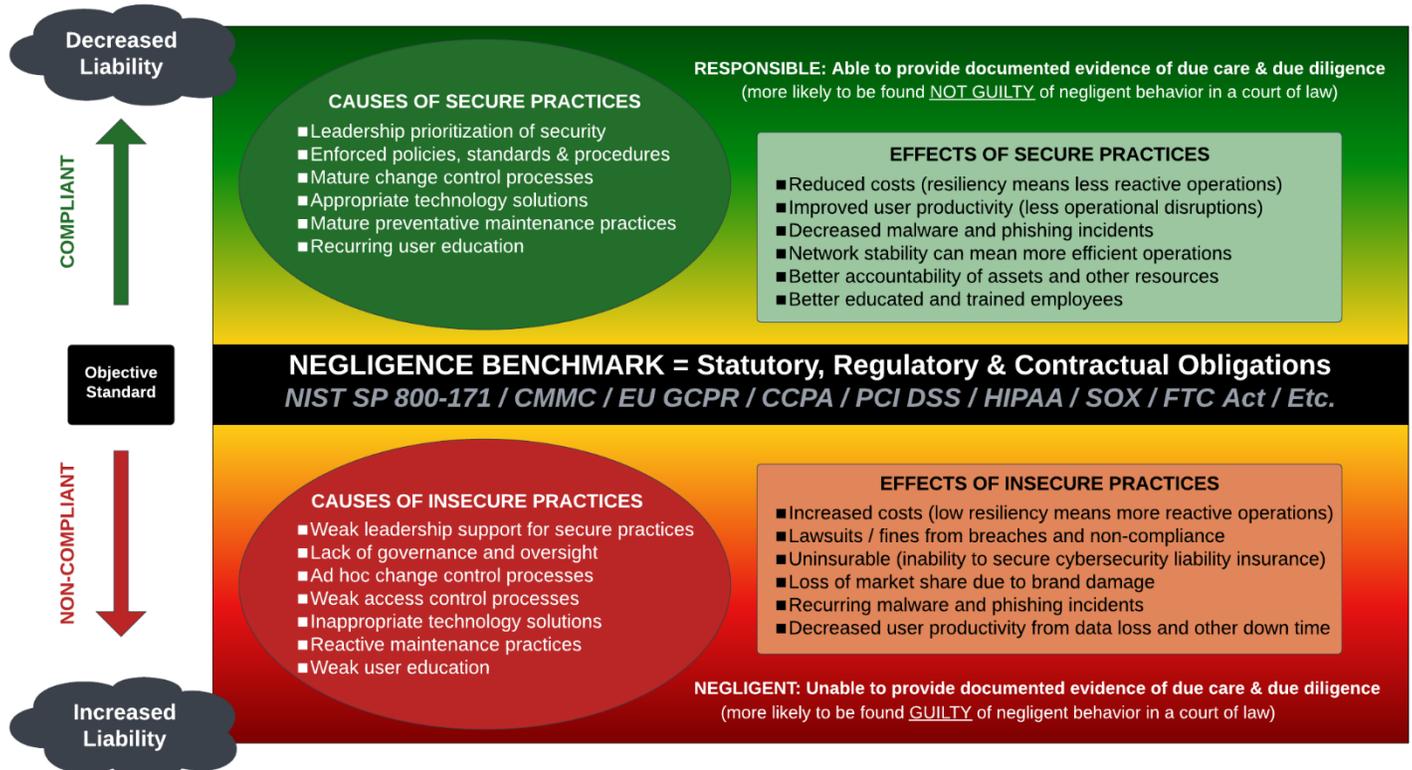
BUSINESS PLANNING CONSIDERATIONS: AVOIDING NEGLIGENCE

It is important to understand the goals for business planning and one of those is to avoid being considered negligent. The Legal Information Institute (LII) defines negligence as *“a failure to behave with the level of care that someone of ordinary prudence would have exercised under the same circumstances.”*⁵

The “level of care that someone of ordinary prudence” would perform entails the use of industry-recognized practices (e.g., CMMC, NIST SP 800-171, HIPAA, PCI DSS, ISO 27002, etc.). For many organizations, it is very clear what the minimum requirements are (e.g., NIST SP 800-171 and PCI DSS). Without a justifiable business reason that addresses the need to deviate from a requirement, non-compliance with those objective benchmarks may be considered negligent behavior. It is important to note that both businesses and individuals may be legally and financially liable for injuries caused due to negligence.

Negligence is situationally dependent. For example, an intoxicated driver who gets behind the wheel is negligent. A negligent driver could in reality be a champion race car driver and is not incompetent in any regard. When sober, that individual may be an excellent driver, but driving intoxicated constitutes a negligent act. Negligence has nothing to do with being incompetent!

⁵ LLI - <https://www.law.cornell.edu/wex/negligence>



There are quite a few reasons to care about this topic, but a few of particular note include:

- With the multitude of government contractors and their service providers having to comply with NIST SP 800-171, the False Claims Act (FCA) is a “go to jail” level offense that impacts both prime and subcontractors. It is also worth noting that whistleblower, or *qui tam*, actions comprise a significant portion of FCA cases that are filed.⁶
- For companies involved in Mergers & Acquisitions (M&A), the purchase price might end up including a future class-action lawsuit along with the assets of the company acquired (e.g., Bank of America’s 2008 purchase of Countrywide Financial).
- Quality cybersecurity and data privacy practitioners want to make a positive impact and work for a company that takes the topics of cybersecurity and data privacy seriously. They tend to not stick around “sick” companies and risk being tainted by long-term association with the brand when it is clear only lip service is applied to implementing appropriate controls.
- Cybersecurity liability insurance policies generally contain loopholes. While these insurance products are marketed as comprehensive protection, insurers generally cover for incidents resulting from singular employee mistakes during the operation of a computer system or in the handling of digital assets, but not from failing to implement appropriate compliance controls on a broader scale. Insurers are in the business to sell policies, not pay out claims.

DEFINING NEGLIGENCE AS IT PERTAINS TO CYBERSECURITY & DATA PRIVACY

The following content is leveraged from Cornell’s Law School Legal Information Institute (LII)⁷ to help provide some additional context to the previous points previously explained.

Negligent conduct may consist of either an act, or an omission to act when there is a duty to do so. Primary factors to consider in ascertaining whether the person’s conduct lacks reasonable care are:

- The foreseeable likelihood that the person’s conduct will result in harm;
- The foreseeable severity of any harm that may ensue; and
- The burden of precautions to eliminate or reduce the risk of harm.

Four (4) elements are generally required to establish a *prima facie* case of negligence:

1. Existence of a legal duty that the defendant owed to the plaintiff (e.g., *complying with NIST SP 800-171 to protect*

⁶ US Department of Justice - <https://www.justice.gov/opa/pr/justice-department-s-false-claims-act-settlements-and-judgments-exceed-56-billion-fiscal-year>

⁷ Cornell’s Law School - <https://www.law.cornell.edu/wex/negligence>

Controlled Unclassified Information (CUI));

2. Defendant's breach of that duty (e.g., *failure to protect CUI in accordance with NIST SP 800-171 requirements under applicable DFARS clauses*);
3. Plaintiff's suffering of an injury (e.g., *financial losses due to lost contract due to non-compliance with NIST SP 800-171*); and
4. Proof that defendant's breach caused the injury (e.g., *publicity about the data breach or other evidence pointing to the entity being the source of the data breach*)

Typically, to meet the injury element of the *prima facie* case, the injury must be one (1) of two (2) things:

1. Bodily harm; or
2. Harm to property (can be personal property or business property (physical or digital)).

DETERMINING A BREACH OF DUTY

When determining how whether the defendant has breached a duty, courts will usually use the *Learned Hand formula*⁸, which is an algebraic approach to determining liability. If $B < PL$, then there will be negligence liability for the party with the burden of taking precautions where:

- B = Burden of taking precautions
- P = Probability of loss
- L = Gravity of loss

If the burden of taking such precautions is less than the probability of injury multiplied by the gravity of any resulting injury, then the party with the burden of taking precautions will have some amount of liability.

DETERMINING WHETHER THERE WAS A DUTY TO ACT

Typically, if the defendant had a duty to act, did not act (resulting in a breach of duty) and that breach of duty caused an injury, then the defendant's actions will be classified as misfeasance. There are several ways to determine whether the defendant had a duty to act (note: this is not an exhaustive list):

- The defendant engaged in the creation of the risk which resulted in the plaintiff's harm;
- The defendant volunteered to protect the plaintiff from harm;
- The defendant knew / should have known that the conduct will harm the plaintiff; or
- Business/voluntary relationships.

⁸ *Learned Hand Formula* - <https://academic.oup.com/lpr/article/5/1/1/990799>

APPLYING THE CONCEPTS OF ASSURANCE, CONFORMITY & MATERIALITY TO RISK MANAGEMENT

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

ASSURANCE LEVELS: DEFINING CRITERIA FOR RIGOR IN ASSESSING RISK

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.”*⁹ 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:

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

The application of each assessment 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.

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.

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.

[Appendix A: Assessment Rigor](#) covers the details about assessment methods for each of these levels.

⁹ NIST Glossary - <https://csrc.nist.gov/glossary/term/assurance>

CONFORMITY: DEFINING A RISK DETERMINATION

When an organization goes through some form of “certification” process, it undergoes a conformity assessment (e.g., ISO 27001, CMMC, SOC 2, PCI DSS, RMF, etc.). Conformity assessments are designed to assure that a particular product, service, or system meets a given level of quality or safety. **Instead of 100% pass criteria, conformity assessments rely on the concept of assurance to establish a risk-based threshold to determine if the intent of the objective(s) has been achieved.**

This concept of conformity is relevant as it pertains to how to appropriately message risk assessment findings, since risk management requires educating stakeholders for situational awareness and decision-making purposes. There are many options and formats available to report the results of a risk assessment, but this can be considered a Report on Conformity (ROC). The reason for this is a risk assessment is evaluating if an organization’s cybersecurity and data privacy practices conform to its stated risk tolerance.

During a risk assessment, controls can be assessed as one (1) of four (4) findings:

1. Satisfactory;
2. Deficient;
3. Not Applicable; or
4. Compensating Control (e.g., compensating control).

This approach can be summarized by reporting to the organization management on the “health” of the assessed controls by one (1) of four (4) following risk determinations:

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

RISK DETERMINATION: STRICTLY CONFORMS

The risk determination of Strictly Conforms is a positive outcome. Strictly Conforms indicates:

1. The organization 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:
 - a. The controls are met and operational;
 - b. Any control designated as Not Applicable (N/A) is validated as such by the assessor; and/or
 - c. Where applicable, compensating controls are validated by the assessor as being:
 - i. Applicable;
 - ii. Reasonable; and
 - iii. Implemented and operating properly; and
2. Assessed controls provide reasonable assurance that the organization’s cybersecurity and data protection program provides adequate security, where it:
 - a. Adheres to a defined and documented risk tolerance;
 - b. Mitigates material cybersecurity and/or data protection risks;
 - c. Is designed to detect and protect against material cybersecurity and/or data protection threats; and
 - d. Is prepared to respond to material incidents.

A statement that the assessed controls STRICTLY CONFORMS indicates to the organization management that sufficient evidence of due care and due diligence exists to provide assurance that the organization’s stated risk tolerance is achieved.

RISK DETERMINATION: CONFORMS

The risk determination of Conforms is a positive outcome. Conforms indicates:

1. The organization 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:
 - a. The controls are met and operational;
 - b. Any control designated as N/A is validated as such by the assessor; and/or
 - c. Where applicable, compensating controls are validated by the assessor as being:
 - i. Applicable;
 - ii. Reasonable; and
 - iii. Implemented and operating properly;
2. Any assessed control deficiency is not material to the organization's cybersecurity and data protection program; and
3. Assessed controls provide reasonable assurance that the organization’s cybersecurity and data protection program

provides adequate security, where it:

- a. Adheres to a defined and documented risk tolerance;
- b. Mitigates material cybersecurity and/or data protection risks;
- c. Is designed to detect and protect against material cybersecurity and/or data protection threats; and
- d. Is prepared to respond to material incidents.

A statement that the assessed controls CONFORMS indicates to the organization management that sufficient evidence of due care and due diligence exists to provide assurance that the organization's stated risk tolerance is achieved.

RISK DETERMINATION: SIGNIFICANT DEFICIENCY

The risk determination of Significant Deficiency is a negative outcome. Significant Deficiency indicates:

1. The organization 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:
 - a. At least seventy percent (70%), but less than eighty percent (80%), of the assessed controls have reasonable evidence to conclude:
 - i. The controls are met and operational;
 - ii. Any control designated as N/A is validated as such by the assessor; and/or
 - iii. Where applicable, compensating controls are validated by the assessor as being:
 1. Applicable;
 2. Reasonable; and
 3. Implemented and operating properly;
2. Any assessed control deficiency is not material to the organization's cybersecurity and data protection program;
3. Assessed controls do not provide reasonable assurance that the organization's cybersecurity and data protection program provides adequate security, where it:
 - a. Adheres to a defined and documented risk tolerance;
 - b. Mitigates material cybersecurity and/or data protection risks;
 - c. Is designed to detect and protect against material cybersecurity and/or data protection threats; and
 - d. Is prepared to respond to material incidents; and
4. The organization's cybersecurity and data protection program:
 - a. 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
 - b. Requires implementing limited changes to personnel, technology and/or practices to correct the design and implementation of deficient cybersecurity and/or data protection controls.

A statement that the assessed controls have a SIGNIFICANT DEFICIENCY indicates to the organization management that insufficient evidence of due care and due diligence exists to provide assurance that the organization's stated risk tolerance is achieved, due to a systemic problem in the cybersecurity and/or data privacy program.

RISK DETERMINATION: MATERIAL WEAKNESS

The risk determination of Material Weakness is a negative outcome. Material Weakness indicates:

1. The organization 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:
 - a. One (1), or more, material controls is/are deficient; and/or
 - b. Less than seventy percent (70%) of the assessed controls have reasonable evidence to conclude:
 - i. The controls are met and operational;
 - ii. Any control designated as N/A is validated by the assessor and confirmed as such; and/or
 - iii. Where applicable, compensating controls are validated by the assessor as being:
 1. Applicable;
 2. Reasonable; and
 3. Implemented and operating properly;
2. Assessed controls do not provide reasonable assurance that the organization's cybersecurity and data protection program adequately:
 - a. Adheres to a defined and documented risk tolerance;
 - b. Mitigates material cybersecurity and/or data protection risks; and/or
 - c. Possesses the capability to:
 - i. Detect and protect against material cybersecurity and/or data protection threats; and/or
 - ii. Respond to material incidents; and

3. The organization's cybersecurity and data protection program:
 - a. Cannot perform its stated mission; and
 - b. Drastic changes to people, processes and/or technologies are required to remediate the deficiencies.

A statement that the assessed controls have a MATERIAL WEAKNESS indicates to the organization's management that deficiencies are grave enough that it 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. Essentially, the security and data privacy program are incapable of performing its stated mission and drastic changes to people, processes and/or technology are necessary to remediate the findings.

MATERIALITY: CRITERIA TO ESTABLISH RISK THRESHOLDS

The Secure Controls Framework (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.”*¹⁰

In an effort to avoid Garbage In, Garbage Out (GIGO) risk management practices, materiality designations can help determine what constitutes reasonable assurance that an organization adheres to its stated risk tolerance. This is where clear findings are useful to understand and report on the health of a cybersecurity and data privacy program:

- Strictly Conforms;
- Conforms;
- Significant Deficiency; or
- Material weakness.

Materiality provides relevant context to risk thresholds as compared to 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.

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.”*¹¹
- 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.”*¹²

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.

COMMON MATERIALITY THRESHOLDS

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:¹³

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

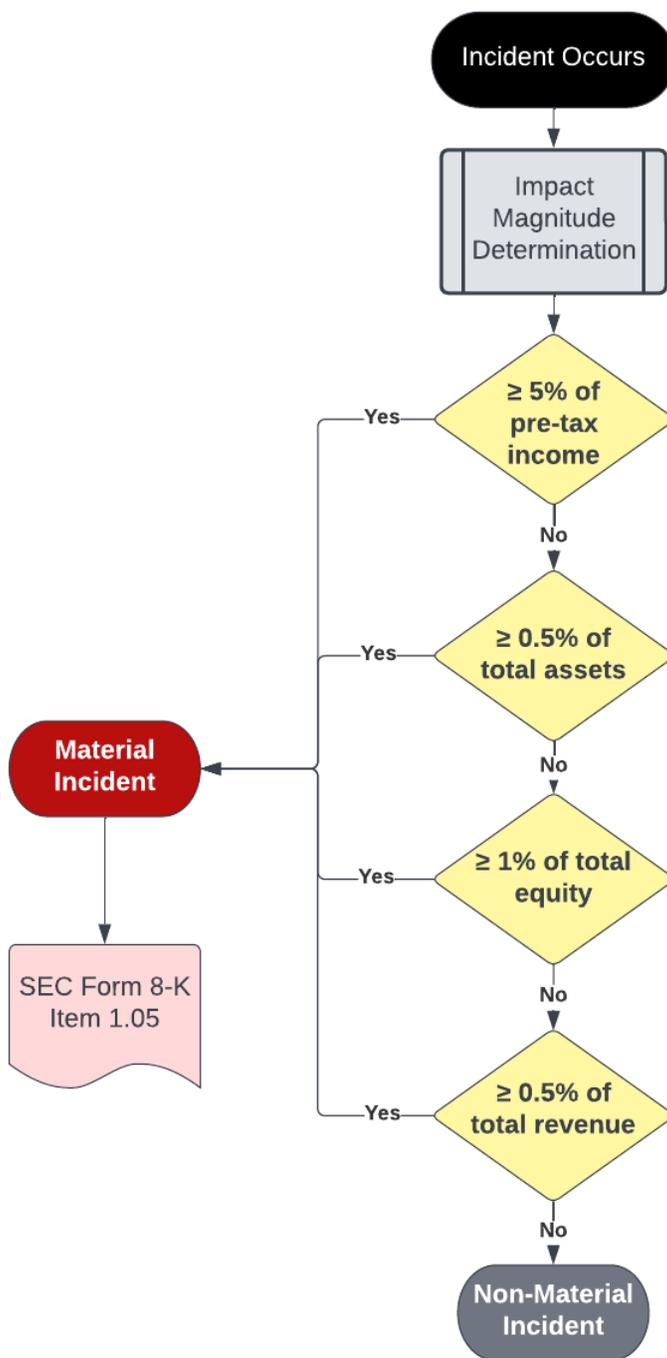
¹⁰ SCF Cybersecurity Materiality - <https://securecontrolsframework.com/cybersecurity-materiality/>

¹¹ SEC - <https://www.sec.gov/comments/265-24/26524-77.pdf>

¹² IFRS - <https://www.ifrs.org/content/dam/ifrs/project/definition-of-materiality/definition-of-material-feedback-statement.pdf>

¹³ Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf

This materiality determination can be visualized with this infographic with the callout for publicly traded companies having a requirement to publicly disclose material cybersecurity incidents:¹⁴



¹⁴ SEC Cybersecurity Final Rule - <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

MATERIAL WEAKNESS VS MATERIAL CONTROL VS MATERIAL RISK VS MATERIAL THREAT VS MATERIAL INCIDENT

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

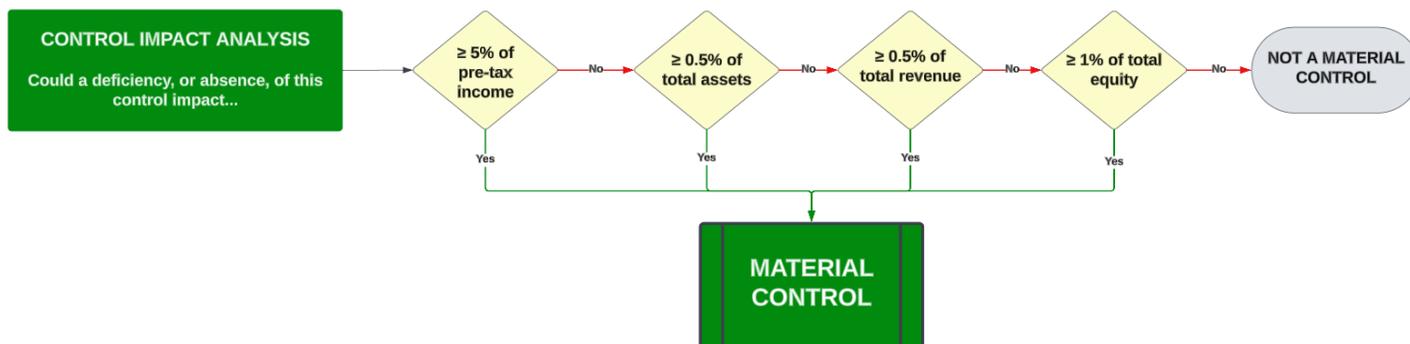
A material weakness is a deficiency, or a combination of deficiencies, in an organization's cybersecurity and/or data privacy controls (across its supply chain) where it is probable that reasonable threats will not be prevented or detected in a timely manner that directly, or indirectly, affects assurance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

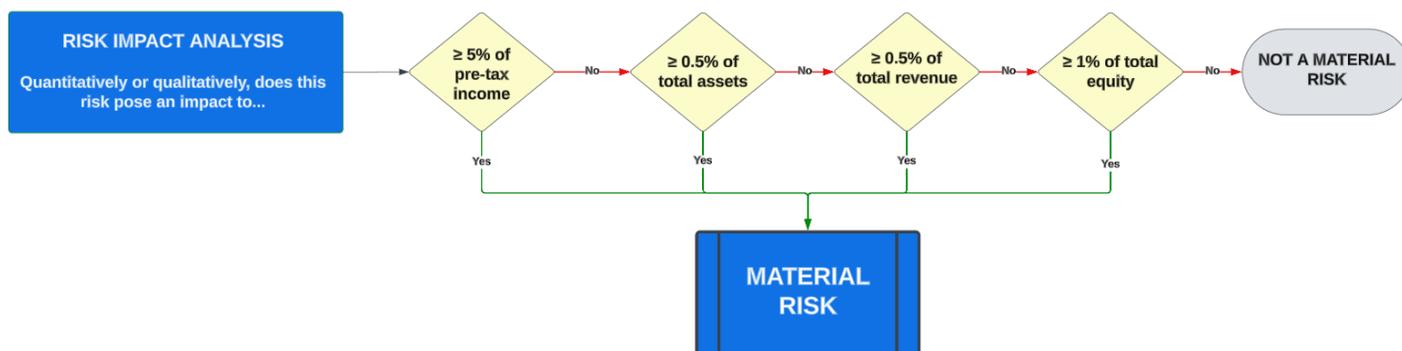
- It is not capable of having compensating controls; and
- Its absence, or failure, exposes an organization to such a degree that it could have a material impact.



MATERIAL RISK

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

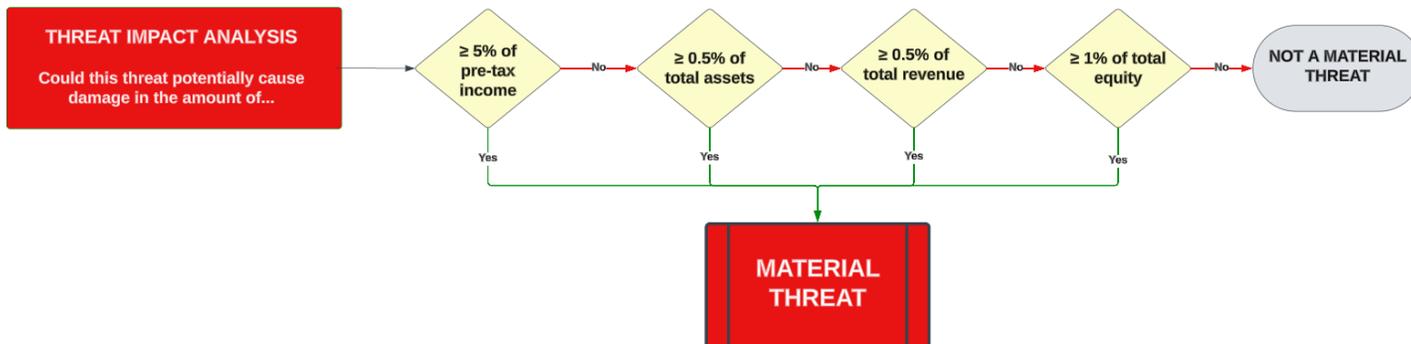
- Is a quantitative or qualitative scenario where the exposure to danger, harm or loss has a material impact (e.g., significant financial impact, potential class action lawsuit, death related to product usage, etc.); and
- Should be identified and documented in an organization's "risk catalog" that chronicles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

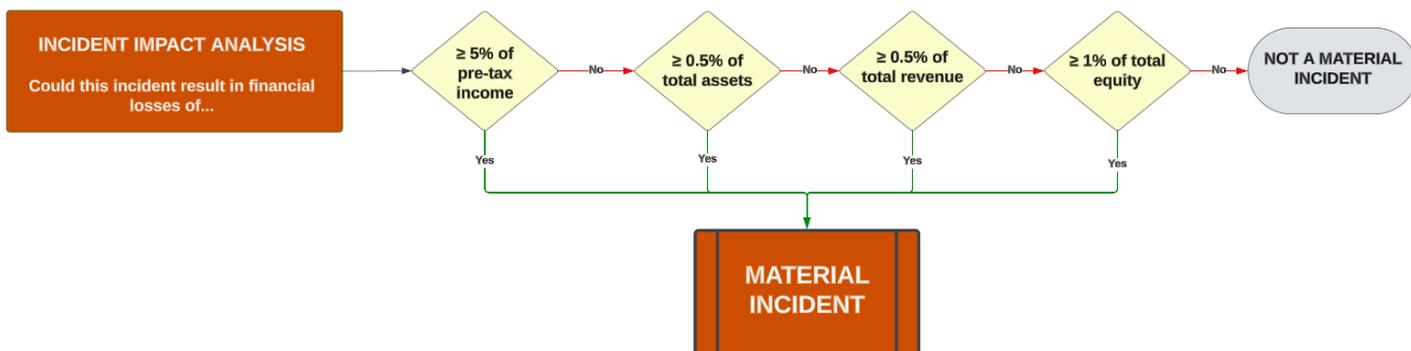
- Is a vector that causes damage or danger that has a material impact (e.g., poorly governed Artificial Intelligence (AI) initiatives, nation state hacking operations, dysfunctional internal management practices, etc.); and
- Should be identified and documented in an organization's "threat catalog" that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



SECURITY & EXCHANGE COMMISSION (SEC) – CYBERSECURITY RISK MANAGEMENT, STRATEGY, GOVERNANCE & INCIDENT DISCLOSURE

The SEC published its Final Rule on cybersecurity risk management, strategy, governance and incident disclosure to comply with Form 8-K Item 1.05 by December 18, 2023.¹⁵ Smaller reporting companies will have an additional 180 days and must begin complying no later June 15, 2024.

DEFINING RISK MANAGEMENT & GOVERNANCE PRACTICES

SEC Regulation S-K Item 106 deals with governance practices. Publicly traded companies (registrants) must publicly describe the following:

- The board of director's oversight of risks from cybersecurity threats; and
- Management's role in assessing and managing material risks from cybersecurity threats.

17 CFR 229.106(B) - RISK MANAGEMENT & STRATEGY

- (1) Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:
 - (i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;
 - (ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
 - (iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.
- (2) Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.¹⁶

17 CFR 229.106(C) - GOVERNANCE

- (1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.
- (2) Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:
 - (i) Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
 - (ii) The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
 - (iii) Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.¹⁷

PUBLIC DISCLOSURE REQUIREMENT FOR CYBERSECURITY INCIDENTS

Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its:

- Nature, scope, and timing; and
- Impact or reasonably likely impact.

FORM 8-K ITEM 1.05 – MATERIAL CYBERSECURITY INCIDENTS

(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.¹⁸

¹⁵ SEC Cybersecurity Final Rule - <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

¹⁶ SEC subpart 229.100 – Business - <https://www.ecfr.gov/current/title-17/chapter-II/part-229/subpart-229.100>

¹⁷ SEC subpart 229.100 – Business - <https://www.ecfr.gov/current/title-17/chapter-II/part-229/subpart-229.100>

¹⁸ Form 8K Item 1.05 - <https://www.sec.gov/files/form8-k.pdf>

Disclosure must be made “without unreasonable delay” through Form 8-K Section 1.05 within four (4) business days after determining that the registrant experienced a material cybersecurity incident. 17 CFR 229.106(a), does define a cybersecurity incident as “an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.” However, the on pages 36-38 of the SEC Final Rule, the SEC further states:

“We (SEC) also decline to use a quantifiable trigger for Item 1.05 because some cybersecurity incidents may be material yet not cross a particular financial threshold.

We note above that the material impact of an incident may encompass a range of harms, some quantitative and others qualitative. A lack of quantifiable harm does not necessarily mean an incident is not material. For example, an incident that results in significant reputational harm to a registrant may not be readily quantifiable and therefore may not cross a particular quantitative threshold, but it should nonetheless be reported if the reputational harm is material. Similarly, whereas a cybersecurity incident that results in the theft of information may not be deemed material based on quantitative financial measures alone, it may in fact be material given the impact to the registrant that results from the scope or nature of harm to individuals, customers, or others, and therefore may need to be disclosed.

In other words, a company being unable to determine the full extent of an incident because of the nature of the incident or the company’s systems, or otherwise the need for continued investigation regarding the incident, should not delay the company from determining materiality.”

REFERENCED FRAMEWORKS & SUPPORTING PRACTICES

This document references numerous leading industry frameworks in an effort to provide a holistic approach to cybersecurity and data privacy-related risk management practices. The following external content is a non-exhaustive list of frameworks that either support the implementation of or are referenced by this document:

- The National Institute of Standards and Technology (NIST):¹⁹
 - NIST SP 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
 - NIST SP 800-39: *Managing Cybersecurity Risk: Organization, Mission and Information System View*
 - NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations*
 - NIST SP 800-64: *Security Considerations in Secure Development Life Cycle*
 - NIST SP 800-122: *Guide to Protecting the Confidentiality of PII*
 - NIST SP 800-161: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*
 - NIST SP 800-171: *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*
 - NIST IR 7298: *Glossary of Key Cybersecurity Terms*
 - NIST Framework for Improving Critical Cybersecurity (NIST Cybersecurity Framework)
- Secure Controls Framework (SCF):
 - Cybersecurity & Data Protection Assessment Standards (CDPAS)²⁰
 - Cybersecurity & Data Privacy Risk Management Model (C|P-RMM)²¹
 - Cybersecurity Materiality²²
- ComplianceForge
 - Hierarchical Cybersecurity Governance Framework (HCGF)²³
 - Integrated Controls Management (ICM)²⁴
- Security and Exchanges Commission (SEC)
 - SEC Cybersecurity Final Rule²⁵
- Norwegian Research Council
 - Current Materiality Guidance for Auditors²⁶

¹⁹ National Institute of Standards and Technology - <https://csrc.nist.gov/publications/sp>

²⁰ SCF CDPAS - <https://securecontrolsframework.com/content/cdpas.pdf>

²¹ SCF SP-RMM - <https://securecontrolsframework.com/risk-management-model/>

²² SCF Cybersecurity Materiality - <https://securecontrolsframework.com/cybersecurity-materiality/>

²³ ComplianceForge HCGF - <https://complianceforge.com/content/Hierarchical-Cybersecurity-Governance-Framework.pdf>

²⁴ ComplianceForge ICM - <https://complianceforge.com/content/Integrated-Controls-Management.pdf>

²⁵ SEC Cybersecurity Final Rule - <https://www.sec.gov/files/rules/final/2023/33-11216.pdf>

²⁶ Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf

APPENDICES

APPENDIX A: ASSESSMENT RIGOR

This assessment rigor comes from the SCF's Cybersecurity & Data Protection Assessment Standards (CDPAS) and is based on assessment methods described in NIST SP 800-172A Appendix C.²⁷ There are three (3) levels of rigor:

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.

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 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 | | <p>Results from examination, interviews and testing are used to support the determination of:</p> <ul style="list-style-type: none"> ▪ Security safeguard existence; ▪ Functionality; ▪ Correctness; ▪ Completeness; and ▪ Potential for improvement over time. <p>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:</p> <ol style="list-style-type: none"> 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. | An interview that consists of broad-based, high-level discussions with individuals or groups of individuals. | A test methodology assumes no knowledge of the internal structure and implementation detail of the assessment object. This methodology is |

²⁷ SCF CDPAS - <https://securecontrolsframework.com/content/cdpas.pdf>

| | | | | |
|--------------------|-----------------------|---|--|---|
| | | <p>This type of examination is conducted using a limited body of evidence or documentation including:</p> <ul style="list-style-type: none"> ▪ Functional-level descriptions for mechanisms; ▪ High-level process descriptions for activities; and ▪ Documents for specifications. | <p>This type of interview is conducted using a set of generalized, high-level questions.</p> | <p>also referred to as “black box” testing.</p> <p>This type of testing is conducted using:</p> <ul style="list-style-type: none"> ▪ A functional specification for mechanisms; and ▪ A high-level process description for activities. |
| Assessment Objects | Specifications | <p>Review:</p> <ul style="list-style-type: none"> ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs. | N/A | N/A |
| | Mechanisms | <p>Review configurations and/or functionality implemented in:</p> <ul style="list-style-type: none"> ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware. | N/A | <p>Test functionality in:</p> <ul style="list-style-type: none"> ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware. |
| | Activities | <p>Review procedures associated with:</p> <ul style="list-style-type: none"> ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises. | N/A | <p>Test applicable procedures for:</p> <ul style="list-style-type: none"> ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.). |
| | Individuals or Groups | N/A | <p>Conduct interviews with applicable stakeholders associated with control execution and/or oversight.</p> <p>Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities:</p> <ul style="list-style-type: none"> ▪ <u>Responsible</u> - People directly responsible for performing a task (e.g., control/process operator); ▪ <u>Accountable</u> - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ <u>Supportive</u> - People under the coordination of the Responsible person for support in performing the task; | N/A |

| | | | | |
|--|--|--|---|--|
| | | | <ul style="list-style-type: none">▪ <u>Consulted</u> - People not directly involved in task execution but were consulted for subject matter expertise; and▪ <u>Informed</u> - People not involved in task execution but are informed when the task is completed. | |
|--|--|--|---|--|

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.

| ENHANCED 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 | | <p>Results from examination, interviews and testing are used to support the determination of:</p> <ul style="list-style-type: none"> ▪ Security safeguard existence; ▪ Functionality; ▪ Correctness; ▪ Completeness; and ▪ Potential for improvement over time. <p>Enhanced rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining whether:</p> <ol style="list-style-type: none"> 1. The applicable controls are: <ol style="list-style-type: none"> a. Implemented; and b. Free of obvious/apparent errors; and 2. There are increased grounds for confidence that the applicable controls are: <ol style="list-style-type: none"> a. Implemented correctly; and b. Operating as intended. | | |
| Attributes | Assessment Depth | <p>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 evidence or documentation.</p> <p>Examples include:</p> <ul style="list-style-type: none"> ▪ Functional-level descriptions and where appropriate and available, high-level design | <p>An interview that consists of broad-based, high-level discussions and more in-depth discussions in specific areas with individuals or groups of individuals.</p> <p>This type of interview is conducted using:</p> <ul style="list-style-type: none"> ▪ A set of generalized, high-level questions; and ▪ More in-depth questions in specific areas where responses indicate a need | <p>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.</p> <p>This type of testing is conducted using:</p> <ul style="list-style-type: none"> ▪ A functional specification and limited system architectural information (e.g., high-level design) for mechanisms and a high- |

| | | | | |
|--------------------|-----------------------|---|---|---|
| | | <p>information for mechanisms;</p> <ul style="list-style-type: none"> High-level process descriptions and implementation procedures for activities; and Documents and related documents for specifications. | for more in-depth investigation. | <p>level process description; and</p> <ul style="list-style-type: none"> A high-level description of integration into the operational environment for activities. |
| Assessment Objects | Specifications | <p>Review:</p> <ul style="list-style-type: none"> Policies; Plans; Procedures; System requirements; and Designs. | N/A | N/A |
| | Mechanisms | <p>Review configurations and/or functionality implemented in:</p> <ul style="list-style-type: none"> Hardware; Software (e.g., services and applications); and Firmware. | N/A | <p>Test functionality in:</p> <ul style="list-style-type: none"> Hardware; Software (e.g., services and applications); and Firmware. |
| | Activities | <p>Review procedures associated with:</p> <ul style="list-style-type: none"> Designs; System operations; Administration; Management; and/or Exercises. | N/A | <p>Test applicable procedures for:</p> <ul style="list-style-type: none"> System operations; Administrative activities; Management functions; and Exercises (e.g., incident response, business continuity, security awareness, etc.). |
| | Individuals or Groups | N/A | <p>Conduct interviews with applicable stakeholders associated with control execution and/or oversight.</p> <p>Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities:</p> <ul style="list-style-type: none"> <u>Responsible</u> - People directly responsible for performing a task (e.g., control/process operator); <u>Accountable</u> - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); <u>Supportive</u> - People under the coordination of the Responsible person for support in performing the task; <u>Consulted</u> - People not directly involved in task | N/A |

| | | | | |
|--|--|--|--|--|
| | | | <p>execution but were consulted for subject matter expertise; and</p> <ul style="list-style-type: none">▪ <u>Informed</u> - 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 | | <p>Results from examination, interviews and testing are used to support the determination of:</p> <ul style="list-style-type: none"> ▪ Security safeguard existence; ▪ Functionality; ▪ Correctness; ▪ Completeness; and ▪ Potential for improvement over time. <p>Comprehensive rigor assessments provide a level of understanding of the administrative, technical and physical cybersecurity and/or data protection measures necessary for determining:</p> <ol style="list-style-type: none"> 1. Whether the applicable controls are: <ol style="list-style-type: none"> a. Implemented; and b. Free of obvious/apparent errors; 2. Whether there are further increased grounds for confidence that the applicable controls are: <ol style="list-style-type: none"> 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 | <p>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.</p> <p>This type of examination is conducted using an extensive body of evidence or documentation including:</p> | <p>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.</p> <p>This type of interview is conducted using:</p> <ul style="list-style-type: none"> ▪ A set of generalized, high-level questions; and | <p>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.</p> <p>This type of testing is conducted using:</p> <ul style="list-style-type: none"> ▪ A functional specification; |

| | | | | |
|--------------------|---------------------|--|--|---|
| | | <ul style="list-style-type: none"> ▪ Functional-level descriptions and where appropriate and available: <ul style="list-style-type: none"> ○ 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. | <ul style="list-style-type: none"> ▪ More in-depth, probing questions in specific areas where responses indicate a need for more in-depth investigation. | <ul style="list-style-type: none"> ▪ 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 | <p>Examinations uses a <u>sufficiently large sample of assessment objects</u> (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:</p> <ul style="list-style-type: none"> ▪ Whether the applicable controls are: <ul style="list-style-type: none"> ○ Implemented; and ○ Free of obvious/apparent errors; ▪ Whether there are further increased grounds for confidence that the applicable controls are: <ul style="list-style-type: none"> ○ 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. | <p>Interviews use a <u>sufficiently large sample of individuals</u> in organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide the level of coverage necessary for determining:</p> <ul style="list-style-type: none"> ▪ Whether the applicable controls are: <ul style="list-style-type: none"> ○ Implemented; and ○ Free of obvious/apparent errors; ▪ Whether there are further increased grounds for confidence that the applicable controls are: <ul style="list-style-type: none"> ○ 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. | <p>Testing uses a <u>sufficiently large sample of assessment objects</u> 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:</p> <ul style="list-style-type: none"> ▪ Whether the applicable controls are: <ul style="list-style-type: none"> ○ Implemented; and ○ Free of obvious/apparent errors; ▪ Whether there are further increased grounds for confidence that the applicable controls are: <ul style="list-style-type: none"> ○ 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. |
| Assessment Objects | Specifications | <p>Review:</p> <ul style="list-style-type: none"> ▪ Policies; ▪ Plans; ▪ Procedures; ▪ System requirements; and ▪ Designs. | N/A | N/A |
| | Mechanisms | <p>Review configurations and/or functionality implemented in:</p> <ul style="list-style-type: none"> ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware. | N/A | <p>Test functionality in:</p> <ul style="list-style-type: none"> ▪ Hardware; ▪ Software (e.g., services and applications); and ▪ Firmware. |

| | | | | |
|--|-----------------------|---|--|---|
| | Activities | <p>Review procedures associated with:</p> <ul style="list-style-type: none"> ▪ Designs; ▪ System operations; ▪ Administration; ▪ Management; and/or ▪ Exercises. | N/A | <p>Test applicable procedures for:</p> <ul style="list-style-type: none"> ▪ System operations; ▪ Administrative activities; ▪ Management functions; and ▪ Exercises (e.g., incident response, business continuity, security awareness, etc.). |
| | Individuals or Groups | N/A | <p>Conduct interviews with applicable stakeholders associated with control execution and/or oversight.</p> <p>Interviews should focus on people and/or teams with RASCI-assigned roles and responsibilities:</p> <ul style="list-style-type: none"> ▪ <u>Responsible</u> - People directly responsible for performing a task (e.g., control/process operator); ▪ <u>Accountable</u> - Person overall responsible for the task being performed and has the authority to delegate the task to others (e.g., control/process owner); ▪ <u>Supportive</u> - People under the coordination of the Responsible person for support in performing the task; ▪ <u>Consulted</u> - People not directly involved in task execution but were consulted for subject matter expertise; and ▪ <u>Informed</u> - People not involved in task execution but are informed when the task is completed. | N/A |