Compliance Decision Making Process (CDMP)

A Practical Approach To Facts, Assumptions, Constraints and Courses of Action (COA)

version 2024.2

TABLE OF CONTENTS

INTRODUCTION

Solving a unique problem is the driving reason for compliance planning processes (e.g., How do I comply with NIST 800-171 R3?).

Compliance with cybersecurity and date protection laws, regulations and contractual obligations requires a proactive approach to be efficient and effective. Proactive compliance can be thought of as having four (4) distinct components, which comes from the broader Military Decision Making Process (MDMP) used by the US military. The common military planning acronym associated with this is DIRT:

1. **D**ecisions;
2. **I**ntent;
3. **R**isk; and
4. **T**riggers.

Getting to the point of making a sound decision is built off of multiple supporting processes. In this document, we co-op concepts from DIRT & MDMP with a cybersecurity compliance-focused Compliance Decision Making Process (CDMP). This document helps define a viable process to tackle compliance-related decision making to minimize risk and cost that your organization is exposed to with cybersecurity & data protection compliance efforts.

COMPLIANCE DECISIONS

There are many compliance-related decisions that organizations face. Decisions are often "forks in the road" where there is a binary option to take one path or the other, but not both. This is where the decisions are expected to be based on compliance intent and risk analysis. Examples of decisions that impact compliance operations include:

- The organization accepts a contract to store, process and/or transmit Controlled Unclassified Information (CUI) as part of a contract with a third party (e.g., government, prime contractor, partner, etc.).
- Action is taken to restructure supporting business processes to support the broader corporate strategy.
- The organization's CUI enclave is onsite in its own segmented environment.

COMPLIANCE INTENT

The compliance intent captures your organization's executive leadership's intent for compliance operations. Decisions should be formed, based on compliance intent. Compliance intent:

- Provides the basis for unity of effort throughout the organization to justify cost/changes necessary to comply.
- Is meant to support the organization's broader mission and strategy.
- Allows stakeholders to gain insight into what is expected of them, what constraints apply, and most importantly, why the compliance operations are being conducted.

UNDERSTANDING OF RISK

A clear understanding of compliance intent directly influences risk analysis. Understanding the nuances of compliance-related risk can lead to better decision making and that can lead to proper technology alignment, less unexpected change, etc. Examples of understanding risk include:

- The organization must avoid business engagements with third parties that store/process/transmit CUI that are not able to obtain and maintain Level 2 Cybersecurity Maturity Model Certification (CMMC).
- While Security Protection Data (SPD) is unlikely to be designated as a CUI category by the US National Archives (NARA), the DoD is unlikely to alter its course that SPD must be protected in a manner that limits technology options.
- The majority of False Claims Act (FCA) submissions are made from insiders (often recently separated individuals), so compliance operations must have appropriate evidence of due diligence and due care to demonstrate the organization's compliance efforts.

COMPLIANCE TRIGGERS

Compliance operations are rarely static. Identifying triggers in the compliance landscape can refine risk management analysis and lead to proper decision making that stays inline with compliance intent. Examples of compliance triggers include:

- NIST released NIST SP 800-171 R3.
- DoD issues a class deviation to remain aligned with NIST SP 800-171 R2.
- 32 CFR § 170.19(c)(2) designates External Service Providers (ESPs) as being considered in scope for CMMC requirements if it meets CUI Asset and/or Security Protection Asset (SPA) criteria (e.g., stores, processes and/or transmits CUI or Security Protection Data (SPD).

CDMP STEP 1: AWARENESS OF COMPLIANCE OBLIGATIONS

Substeps:

1. Establish a formal project to resource and manage the compliance process.
2. Conduct an initial assessment of the compliance mandate.
3. Determine the compliance intent.
4. Define the initial scope of compliance.
5. Identify applicable stakeholders.
6. Conduct a gap assessment.
7. Issue preliminary requirements guidance (including facts and assumptions) to stakeholders.
8. Monitor for evolving requirements / changes to compliance requirements.

Inputs:

- Source requirements (e.g., specific law, regulation and/or contractual obligation).
- Operational authority to conduct compliance operations within the organization.
- Documented roles and responsibilities.
- Understanding of risk (e.g., risk appetite, risk tolerance, risk threshold, materiality, etc.)[1]
- Documented stakeholders.

Outputs:

- Project plan (including running estimate for timeline and budget).
- Running Estimate
- Preliminary stakeholder guidance on compliance requirements.

From a broader *"How do I approach compliance?"* perspective, the Integrated Controls Management (ICM) model is an excellent resource to build a viable Governance, Risk & Compliance (GRC) function that follows a Plan, Do, Check & Act (PDCA) methodology.[2] ICM is a "how to GRC playbook" that is meant to help an organization not only comply with legal obligations, but to identify and govern those cybersecurity and data protection controls that will make their operations secure. Being both secure and compliant is the ideal goal for every organization and the ICM provides a roadmap to achieve it.

INITIAL ASSESSMENT (INTERNAL TO COMPLIANCE TEAM)

The initial assessment helps compliance staff determine:

- Time available from notification of compliance obligation to the compliance deadline.
- The compliance staff's Subject Matter Expertise (SME) with the DFARS requirements (e.g., NIST SP 800-171 & CMMC).
- The reasonable scope of the compliance efforts.
- Which consultants and/or External Service Providers (ESP) require contact and incorporation into the planning process.

RUNNING ESTIMATE (SHARED WITH STAKEHOLDERS)

Running estimates helps stakeholders with understanding the situation, assessing progress and making effective decisions throughout compliance operations. Effective compliance plans and successful executions hinge on current and accurate running estimates with relevant information. A running estimate contains:

- Identify facts (initial).
- Identify assumptions (initial).
- Organizational status, including third-parties that affect compliance efforts (e.g., gap assessment results).
- Organizational / third-party capabilities (initial assessment).
- Organizational / third-party constraints (initial assessment).
- Initial conclusions and preliminary recommendations with associated risk.

---

[1] *Cybersecurity Risk Management – Practitioner's Guide* - https://complianceforge.com/content/pdf/cybersecurity-practitioners-guide-to-risk-management.pdf

[2] *ICM* - https://complianceforge.com/content/pdf/complianceforge-integrated-controls-management.pdf

CDMP SEPT 2: IDENTIFY FACTS & ASSUMPTIONS

Substeps:

1. Determine facts that affect compliance operations.
2. Determine assumptions that affect compliance operations.

Inputs:

- Initial Assessment
- Running Estimate

Outputs:

- Facts
- Assumptions

It is imperative to separate facts from assumptions.

FACTS

Facts are statements of truth, or statements thought to be true.

For example:

- *The organization stores and processes Controlled Unclassified Information (CUI) as part of a government contract.*
- *NIST SP 800-171 compliance has been a requirement since 1 January 2018.*
- *NIST SP 800 171 R3 was released on 14 May 2024.*
- *The DoD issued a class deviation to delay DFARS implementation of NIST SP 800-171 R3.*
- *Office of Management and Budget (OMB) requires organizations to adopt the most current version of NIST one year after its release.*
- *Per 32 CFR § 170.19(c)(2), an External Service Provider (ESP) will be considered in scope for CMMC requirements if it meets CUI Asset and/or Security Protection Asset (SPA) criteria (e.g., stores, processes and/or transmits CUI or Security Protection Data (SPD).*

ASSUMPTIONS

Assumptions are essentially gaps in knowledge or information that need to be confirmed or denied.

For example:

- *Before NIST SP 800-171 R2 is deprecated in May 2025, the DoD will remove the class deviation for DFARS to transition to NIST SP 800-171 R3.*
- *The DoD may realize that the Defense Industrial Base (DIB) would be under undo financial pressure to adjust its technologies, ESP and business processes to treat SPD as CUI.*

Transitioning assumptions to facts is the goal during planning, as it builds situational understanding and validates planning efforts. Presumptive planning is acceptable, if stakeholders understand the planning is based on assumptions. Compliance staff may continue to plan with assumptions to avoid hindering planning efforts or degrade timelines. To determine risk, when assumptions are involved, compliance staff are expected to use:

- Historical data;
- Intuitive analysis; and/or
- Judgment.

CDMP Step 3: Define a Problem Statement

Substeps:

1. Determine the difference between the current state of the operational environment and desired state.
2. Determine what is preventing the organization from reaching the desired end state.

Inputs:

- Initial Assessment
- Running Estimate
- Facts & Assumptions

Outputs:

- Problem Statement

Problem Statement

Solving a unique problem is the driving reason for compliance planning processes. Problem statement development begins with identifying the problem. To identify the problem, it requires compliance staff to determine answers to two questions:

3. What is the difference between the current state of the operational environment and desired state?
4. What is preventing the organization from reaching the desired end state?

The problem statement is a concise statement of the obstacles preventing an organization from achieving a desired end state. The problem statement should include only the significant elements of the problem framing. In this way, the problem statement becomes concise, yet remains relevant to the rest of the problem-solving process.

An example problem statement might be:

How does EXAMPLE COMPANY adjust its business operations and adopt the right technologies to comply with the US Department of Defense's (DoD's) Cybersecurity Maturity Model Certification (CMMC)?

- *The requirements are numerous and constrict the ability of EXAMPLE COMPANY's internal business units to share data with necessary stakeholders.*
- *EXAMPLE COMPANY has three (3) IT and one (1) cybersecurity personnel on staff, so staffing strength is limited.*
- *Not all existing technologies in use at EXAMPLE COMPANY meet the rigorous compliance requirements.*
- *EXAMPLE COMPANY is receiving pressure from its vendors to demonstrate compliance with CMMC, where a failure to demonstrate compliance, or a viable path to compliance, will result in cancelled contracts.*

CDMP Step 4: Determine Constraints

Substeps:

1. Determine resourcing limitations.
2. Determine technical limitations.
3. Determine conflicting business processes.

Inputs:

- Initial Assessment
- Running Estimate
- Facts & Assumptions
- Problem Statement

Outputs:

- Constraints

A constraint is a restriction placed on compliance efforts, generally from either (1) a technical limitation or (2) a conflicting business practice. A constraint dictates an action, inaction or technical limitation that affects compliance efforts.

There is never enough money, people or time for cybersecurity-related compliance operations. Therefore, it is necessary to clearly identify the applicable constraints that affect compliance operations. This includes, but is not limited to:

- Budgetary resources.
- Available personnel with sufficient subject matter expertise.
- Timeline.
- Technical limitations.
- Existing contractual obligations.

Technical Limitations

Technical limitations are going to be specific to the law, regulation and/or contractual obligation. There may be systems, applications and/or processes that are unable to meet configuration requirements.

For example:

- *An old manufacturing computer that uses an unsupported operating system. It is incapable of being patched or run the latest antimalware software.*
- *A firewall that is able to use AES-256 encryption, which is secure, but does not use a FIPS 140-2 validated cryptographic module.*

Conflicting Business Practice

Conflicting business practices may address the ability to control the environment where sensitive / regulated data is stored, processed and/or transmitted. Conflicting business practices generally lead to expanded compliance scopes.

For example:

- *Sensitive / regulated data is emailed via the corporate email system.*
- *Lack of visitor control through the manufacturing building.*
- *Remote / work from anywhere workforce.*
- *The use of contractors to perform work on projects with sensitive / regulated data.*

CDMP STEP 5: IDENTIFY POSSIBLE COURSES OF ACTION (COA)

Substeps:
1. Analyze compliance intent.
2. Analyze facts, assumptions and constraints.
3. Determine decision points / triggers.

Inputs:
- Initial Assessment
- Running Estimate
- Facts & Assumptions
- Problem Statement
- Constraints

Outputs:
- COAs

The US military defines a Course of Action (COA) as a *"broad potential solution to an identified problem."* Practically, determining a course of action is based on making an educated guess that is derived from available facts, assumptions and constraints. This does not make the process of determining COAs wrong, but it is something that decision makers must fully understand since risk can never be eliminated from the equation when there is a certain level of uncertainty that must be accounted for.

In the development of COAs is often helped by creating a unique COA for each of these questions:
1. What scenario reflects the most advantageous outcome?
2. What scenario reflects the most disadvantageous outcome?
3. What scenarios are plausible that should not be discounted?

Part of COA development involves clearly defining both the advantages and disadvantages of each scenario.

ADVANTAGES

Listing advantages of a particular COA is important for decision makers, but it is important for those developing the COAs to avoid skewing the benefits to meet a preferred narrative. While it is impossible to completely eliminate bias, it is crucial to be as objective as possible in the analysis of advantages.

For example:
- *No requirement to change EXAMPLE COMPANY's technology and/or third-parties.*
- *Ability to drastically reduce the scope of compliance.*

DISADVANTAGES

Listing disadvantages of a particular COA is important for decision makers, but it is important for those developing the COAs to avoid skewing the negatives to meet a preferred narrative. While it is impossible to completely eliminate bias, it is crucial to be as objective as possible in the analysis of disadvantages.

For example:
- *Significant cost and time delay to change EXAMPLE COMPANY's technology and/or third-parties.*
- *Expansion of the scope of compliance.*

CDMP Practical Example (NIST 800-171 Compliance)

The following is a practical example of using the CDMP to address compliance with NIST 800-171 by defining a problem statement and establishing facts, assumptions and constraints to come up with Courses of Action (COA). The intent is for the COA to presented to the example company's leadership team, so that a decision can be made about how to best move forward.

Problem Statement

Per the Cybersecurity Maturity Model Certification (CMMC) Final Rule (32 CFR Part 170), an External Service Provider (ESP) is considered in scope for CMMC requirements if it meets Controlled Unclassified Information (CUI) Asset and/or Security Protection Asset (SPA) criteria (e.g., stores, processes and/or transmits (S/P/T) CUI or Security Protection Data (SPD). Per DFARS 252.204-7012(b)(2)(ii)(D), if EXAMPLE COMPANY intends to use a Cloud Service Provider (CSP) to S/P/T any Covered Defense Information (CDI) in performance of its contract, EXAMPLE COMPANY must ensure its CSPs are either:

1. FedRAMP certified; or
2. Meet security requirements equivalent to the FedRAMP moderate baseline.

How does EXAMPLE COMPANY adjust its business operations and adopt the right technologies to comply with the US Department of Defense's (DoD's) Cybersecurity Maturity Model Certification (CMMC) for SPA & SPD?

- The requirements are numerous and constrict the ability of EXAMPLE COMPANY's internal business units to share data with necessary stakeholders.
- EXAMPLE COMPANY has three (3) IT and one (1) cybersecurity personnel on staff, so staffing strength is limited.
- Not all existing technologies in use at EXAMPLE COMPANY meet the rigorous compliance requirements.
- EXAMPLE COMPANY is receiving pressure from its vendors to demonstrate compliance with CMMC, where a failure to demonstrate compliance, or a viable path to compliance, will result in cancelled contracts.
- An EXAMPLE COMPANY executive will be required to make an annual affirmation in Supplier Performance Risk System (SPRS).

Facts

- EXAMPLE COMPANY S/P/T CUI as part of a government contract.
- NIST SP 800-171 compliance has been a requirement since 1 January 2018.
- NIST SP 800 171 R3 was released on 14 May 2024.
- The DoD issued a class deviation to delay DFARS implementation of NIST SP 800-171 R3.
- Office of Management and Budget (OMB) Circular A-130 requires organizations to adopt the most current version of NIST one year after its release.
- Per 32 CFR § 170.19(c)(2), an External Service Provider (ESP) will be considered in scope for CMMC requirements if it meets CUI Asset and/or Security Protection Asset (SPA) criteria (e.g., stores, processes and/or transmits CUI or Security Protection Data (SPD).
- EXAMPLE COMPANY currently does not treat SPD in the same manner as CUI.
- EXAMPLE COMPANY's current ESPs and CSPs are not:
    - CMMC L2 certified;
    - FedRAMP moderate certified; or
    - FedRAMP moderate equivalent.
- Until the CMMC Final Rule is published, EXAMPLE COMPANY's current compliance requirements for DFARS 252.204-7012 are to document EXAMPLE COMPANY's CUI environment in a System Security Plan (SSP) and track deficiencies per a Plan of Action & Milestones (POA&M).

Assumptions

- Before NIST SP 800-171 R2 is deprecated in May 2025 (per OMB A-130), the DoD will remove the class deviation for DFARS to transition to NIST SP 800-171 R3.
- Before NIST SP 800-171 R3 is enforced, the DoD will release "CMMC 3.0" to address changes from NIST SP 800-171 R3.
- The current technology in use at EXAMPLE COMPANY to S/P/T SPD may not be compliant with the CMMC Final Rule.
- The DoD may realize that the Defense Industrial Base (DIB) would be under undo financial pressure to adjust its technologies, ESP and business processes to treat SPD as CUI.

CONSTRAINTS

- Available ESP and CSP that are capable of S/P/T SPD, per the CMMC Final Rule.
- Budget constraints to re-engineer the CUI environment for (1) new technologies or (2) new third-parties to
- Obtaining FedRAMP certification is not easy. FedRAMP certification generally requires a sponsor (e.g., government client). Approaching FedRAMP certification without a sponsor requires the CSP to through the Joint Authorization Board (JAB) process. The CSP would have to work with a FedRAMP CPAO to get the CSP's evaluated as being in a FedRAMP ready state and then petition the FedRAMP JAB to accept the CSP's authorization package. Given that the JAB process only selects around 12 packages per year, this reduces the odds of unsponsored FedRAMP certification for most CSP.

COURSES OF ACTION (COA)

COA 1: DO NOTHING AND WAIT FOR GUIDANCE.

COA Description: EXAMPLE COMPANY continues addressing applicable NIST SP 800-171 R2 and CMMC 2.0 requirements and does not make any technology / service provider changes until it absolutely has to.

Advantages:

- Short-term minimization of cost / change.

Disadvantages:

- Potential loss of market share to EXAMPLE COMPANY's competitors that are able to earn a CMMC certification before EXAMPLE COMPANY.

COA 2: PERFORM A TECHNOLOGY/SERVICE PROVIDER MIGRATION.

COA Description: EXAMPLE COMPANY takes the CMMC Final Rule at face value, which necessitates changes to how SPA & SPD are treated. This requires new technology investment and potentially new business relationships with third-party vendors.

Advantages:

- Potential marketing win against EXAMPLE COMPANY's competitors who choose to do nothing.
- A potentially more secure environment to protect SPA / SPD.

Disadvantages:

- Limited options for technology solutions and/or compliant CSP/ESP.
- Significant changes to business processes and technology architecture.
- Cost associated with breaking existing contracts / service agreements.
- Effort could be for nothing if the CMMC Final Rule loosens requirements.

COA 3: STICK IT OUT WITH EXISTING TECHNOLOGIES / SERVICE PROVIDERS.

COA Description: EXAMPLE COMPANY takes a guarded "wait and see" approach to the CMMC Final Rule, where EXAMPLE COMPANY will make a reasonable effort to work with existing technologies and CSP/ESP to address changes.

Advantages:

- Short-term minimization of cost / change.
- No short-term costs associated with breaking existing contracts / service agreements.
- EXAMPLE COMPANY's existing technology providers and CSP/ESP will have a vested interest in rapidly evolving their offerings to keep EXAMPLE COMPANY as a client.

Disadvantages:

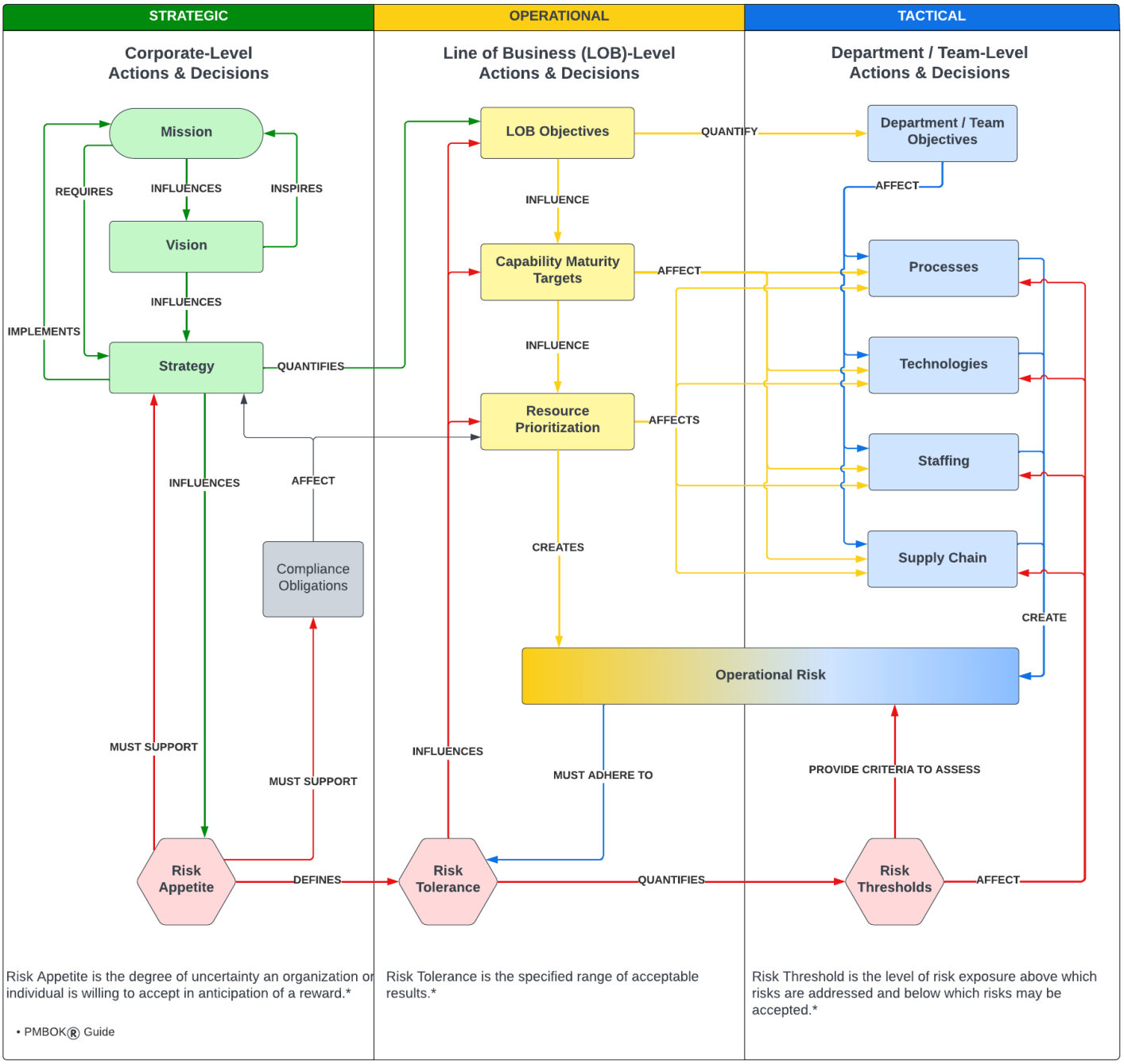
- Potential loss of market share to EXAMPLE COMPANY's competitors that are able to earn a CMMC certification before EXAMPLE COMPANY.

UNDERSTANDING OF RISK: COMPLIANCE DECISION MAKING

The CDMP relies on the understanding that risk management practices exist. To help ensure that coherent risk management discussions can occur, this section is focused on risk management practices.

As visualized in the graphic below, the key concepts of risk management span strategic, operational and tactical layers:

- 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.

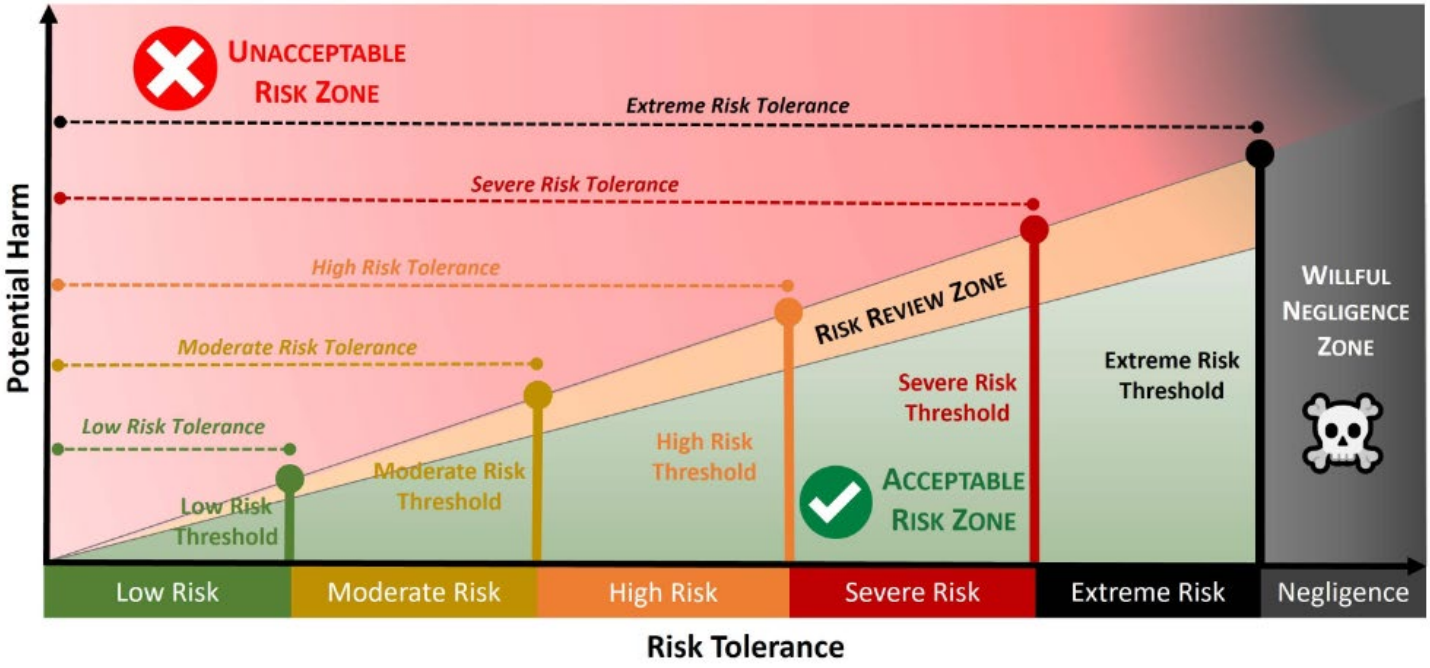


BASELINING RISK MANAGEMENT TERMINOLOGY

Risk management involves coordinated activities that optimize the management of potential opportunities and adverse effects, where the alternative to risk management is crisis management. 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.



WHAT IS A RISK?

In the context of cybersecurity and data privacy 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.*

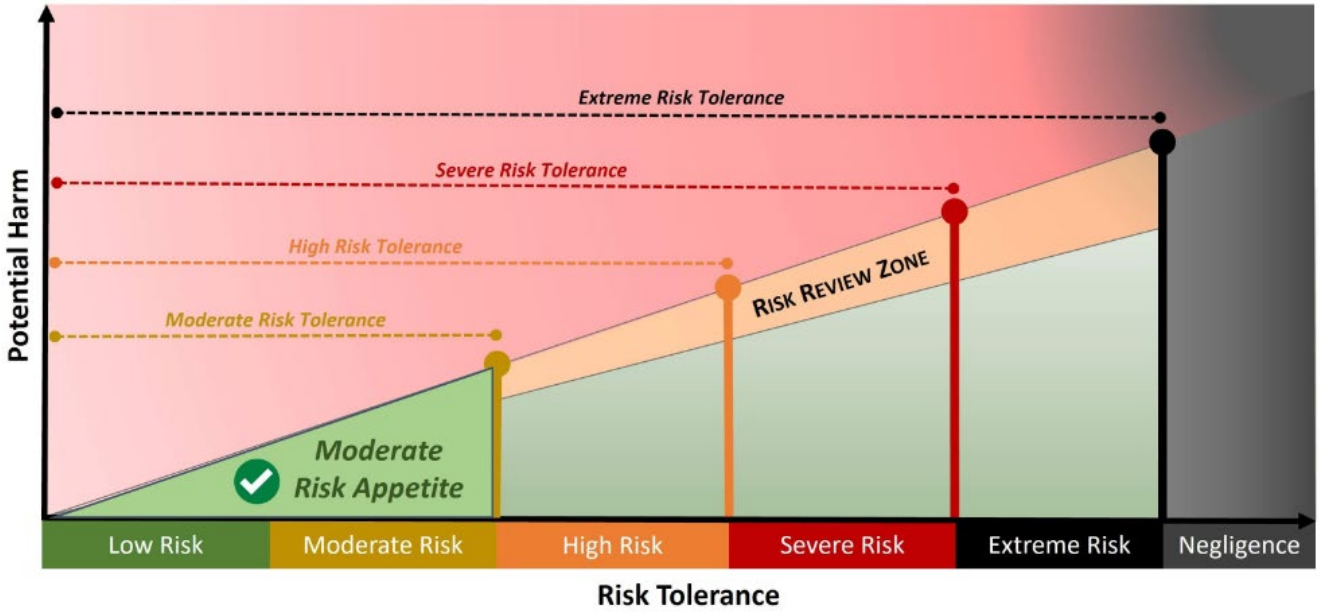
RISK MANAGEMENT OPTIONS

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

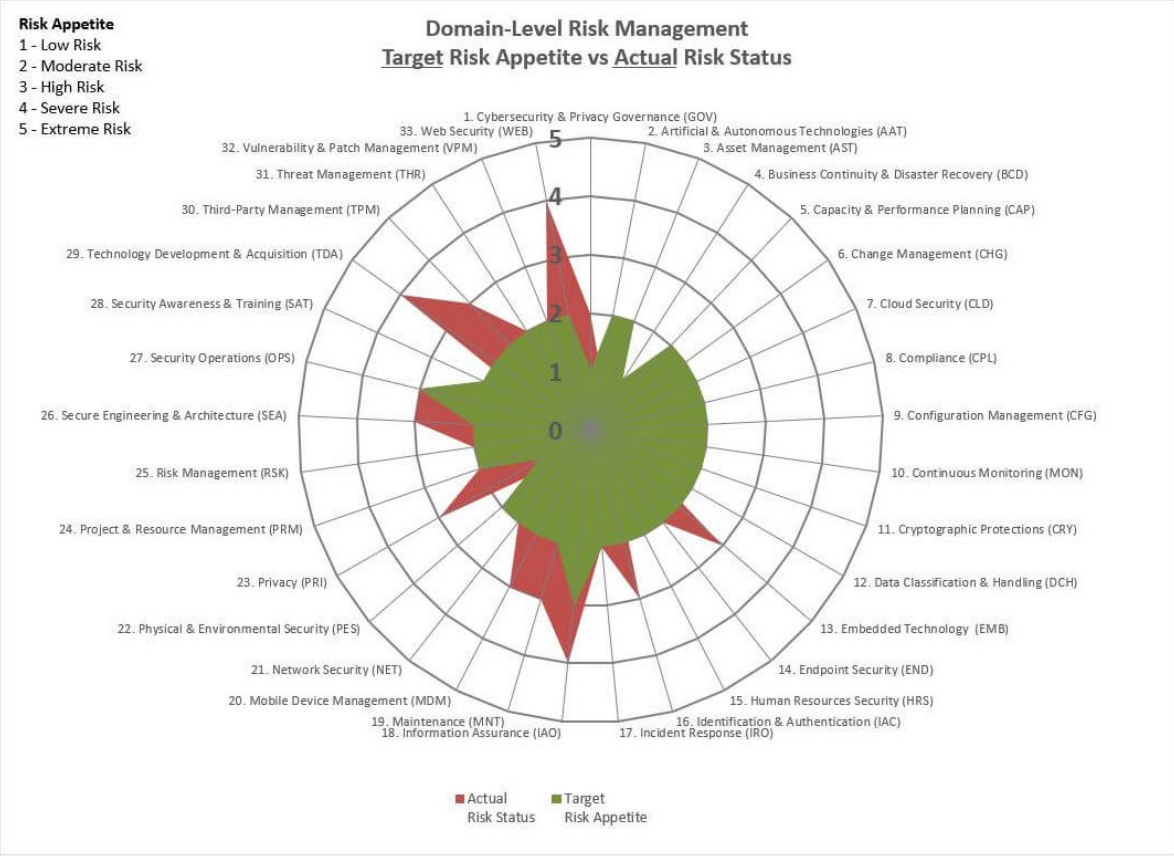
1. Reduce the risk to an acceptable level;
2. Avoid the risk;
3. Transfer the risk to another party; or
4. Accept the risk.

In a mature risk program, the results of risk assessments are evaluated with the organization's risk appetite in mind. 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, this leaves remediation, transferring or avoiding as the remaining three (3) options.

Building upon the graphic from the previous page, when viewed from a risk appetite perspective, for an organization that wants to follow a "moderate risk appetite," that establishes constraints for allowable and prohibited activities, based on the potential harm to the organization:



To provide greater flexibility, as well greater 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. This can be visualized with a spider / radar diagram, as shown below in the example that applies a risk appetite to each of the thirty-three (33) Secure Controls Framework (SCF) domains.



What Is A Threat?

In the context of the cybersecurity and data privacy risk management practices, "threat" is defined as:

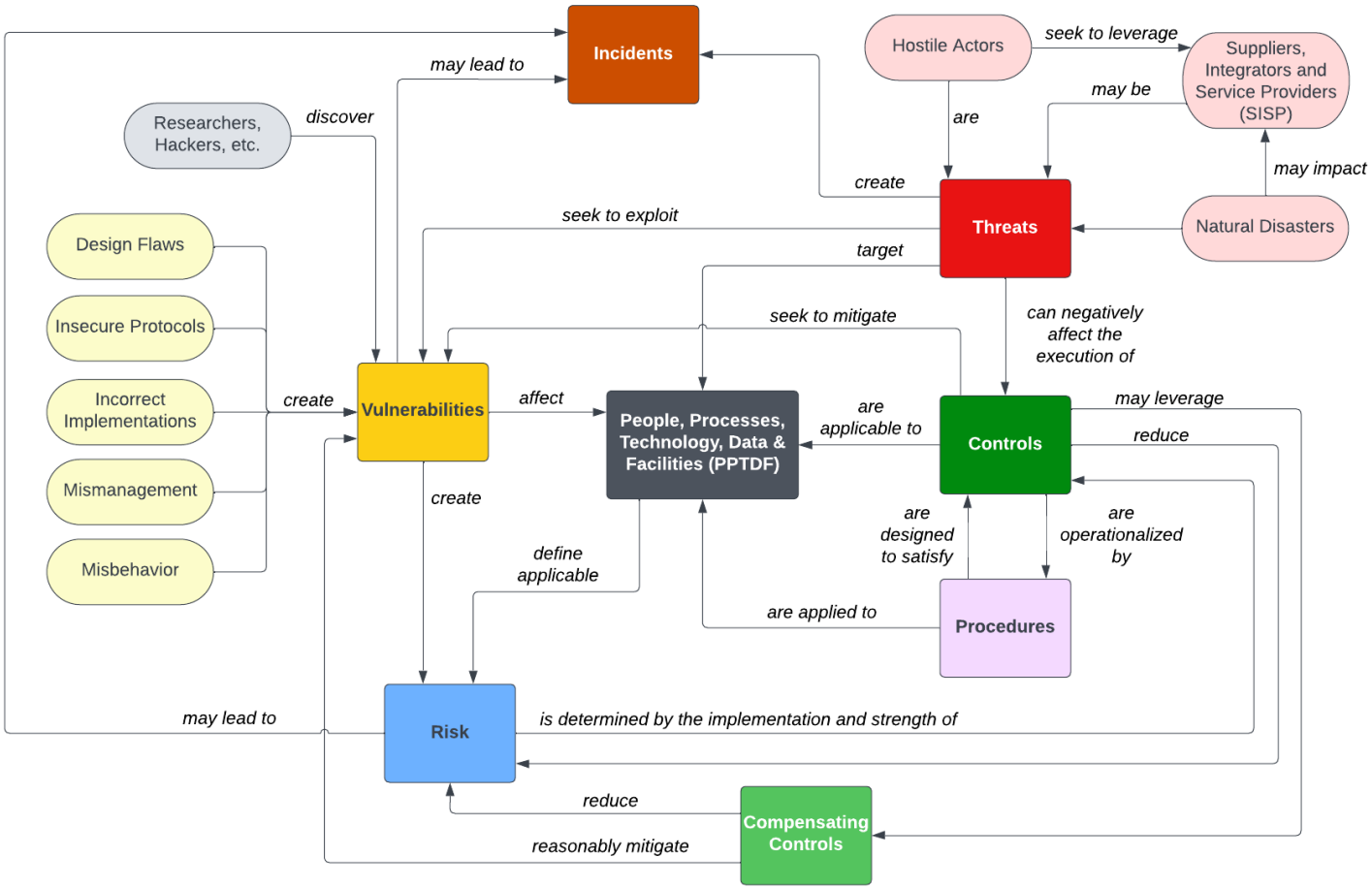
- noun *A person or thing likely to cause damage or danger.*
- verb *To indicate impending damage or danger.*

Understanding The Differences Between 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.

If you want to learn for about threats vs vulnerabilities vs risks, ComplianceForge published a webpage that describes that in greater detail and you can click on the image below for a PDF version.[3]



Risk Tolerance vs Risk Threshold vs Risk Appetite

According to the Project Management Body of Knowledge (PMBOK®) Guide:[4]

- 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.*

[3] *Risk vs Threat vs Vulnerability Ecosystem - https://complianceforge.com/content/pdf/guide-risk-vs-threat-vs-vulnerability-ecosystem.pdf*
[4] *PMBOK® Guide - https://www.pmi.org/pmbok-guide-standards/foundational/pmbok*

Risk Appetite

Risk appetite is more of a management statement, where it is subjective in nature. Similar in concept to how a policy is a "high-level statement of management intent,"[5] an organization's stated risk appetite is a high-level statement of how all, or certain types of, risk are willing to be accepted. Risk appetites exist as a guiderail from an organization's executive leadership to inform personnel about what is and is not acceptable, in terms of risk management. 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.

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

- "EXAMPLE COMPANY is a low-risk organization and will avoid any activities that could harm its customers."
- "EXAMPLE COMPANY 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 profile. Developing breakthrough products and services does invite significant risk through changes to traditional supply chains, disruptions to business operations and changing client demand. Innovation instances that pose greater than a moderate risk will be considered on a case-by-case basis for financial and legal implications."

It is important to know that in many immature risk programs, risk appetite statements are divorced from reality. Executive leaders mean well when they put out 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., MSPs, consultants, vendors, etc.); and
- Lack of pre-production security testing.

Risk Tolerance

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

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

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

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

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

[5] *Hierarchical Cybersecurity Governance Framework - https://complianceforge.com/content/pdf/complianceforge-hierarchical-cybersecurity-governance-framework.pdf*

Risk Matrix		Occurrence Likelihood					
		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	Catastrophic	6	12	18	24	30	36
	Critical	5	10	15	20	25	30
	Major	4	8	12	16	20	24
	Moderate	3	6	9	12	15	18
	Minor	2	4	6	8	10	12
	Insignificant	1	2	3	4	5	6

Risk Appetite (*MediumRisk*)

The six (6) categories of IE are:

1. Insignificant;
2. Minor;
3. Moderate;
4. Major;
5. Critical; and
6. Catastrophic.

The six (6) categories of OL are:

1. Remote possibility;
2. Highly unlikely;
3. Unlikely;
4. Possible
5. Likely; and
6. Almost certain.

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 protection 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 security and 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 protection 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 protection 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 (MSSP), 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 protection 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 protection requirements.
- Do not store, process and/or transmit sensitive/regulated data.
- Lack management support for cybersecurity and data privacy governance practices.
- Do not have cyber-related liability insurance.

Organizations that may choose to operate with a high risk tolerance include, but are not limited to:

- Startups
- Artificial Intelligence (AI) developers

Extreme Risk Tolerance

Organizations that would be reasonably-expected to adopt an extreme risk tolerance generally:

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

Organizations that may choose to operate with a high risk tolerance include, but are not limited to:

- Startups
- Artificial Intelligence (AI) developers

Risk Threshold

Risk thresholds are directly tied to risk tolerance. As the graphic at the top of the page depicts, there is a threshold between the different levels of risk tolerance. By establishing thresholds, it brings the "graduated scale perspective" to life.

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.

Examples of how risk thresholds are unique to each organization include:

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

Practical Risk Management Example

Let's take a look at a theoretical company, that is experimenting with Artificial Intelligence (AI) to strengthen its products and/or services. Its long-standing risk appetite is relatively conservative, where the company draws a hard line that any risk over moderate is unacceptable. Additionally, the company has zero tolerance for any activities that could harm its customers.

Given the changes necessary 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 occurrence likelihood of emergent behaviors 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.

With those results, it is a management decision. What does the CEO / Board of Directors (BoD) do?

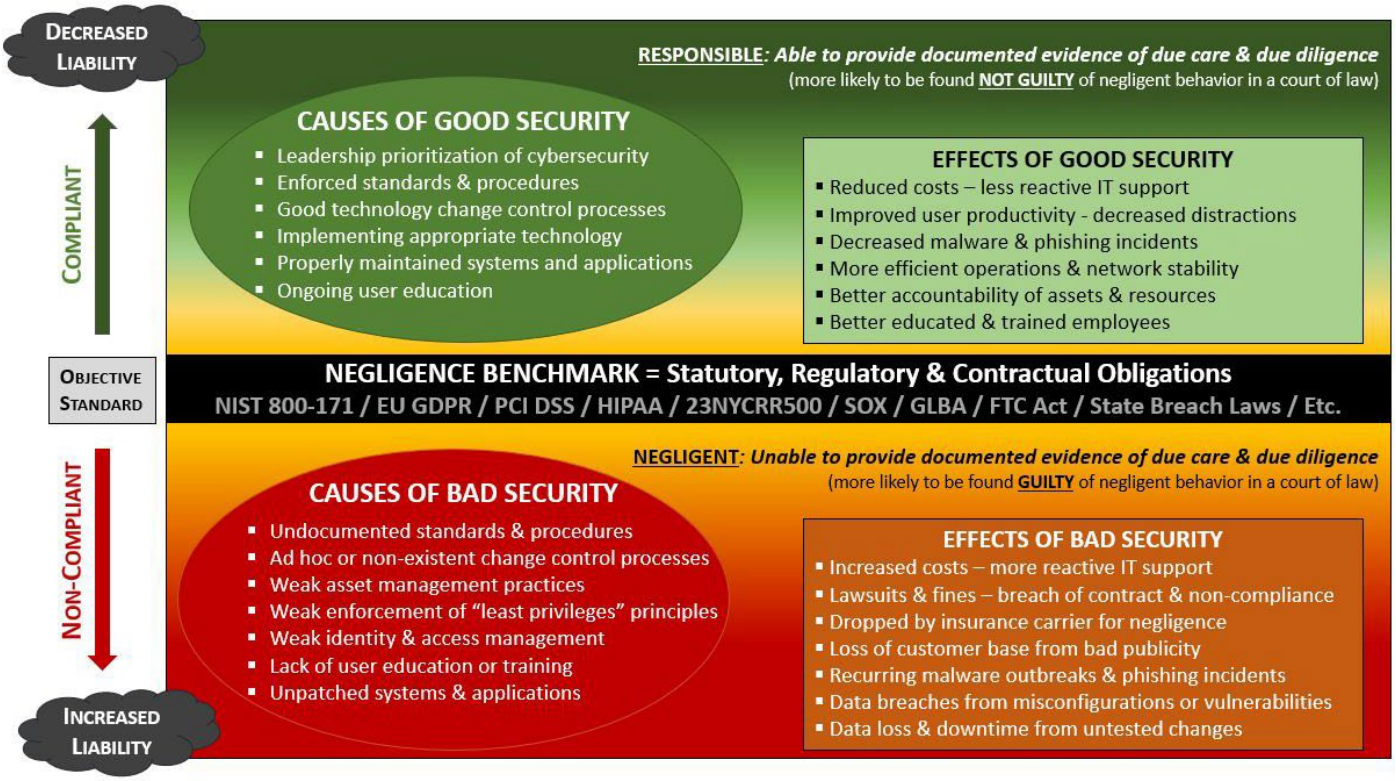
- Dispense with its long-standing risk appetite for this specific project so that a potentially lucrative business opportunity can exist?
- Is the AI project cancelled, due to the level of risk?
- If the CEO/BoD proceeds with accepting the risk, is it violating its fiduciary duties, since it is accepting risk it previously deemed unacceptable? Additionally, would it be considered negligent for accepting 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.

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. Negligence is defined as *"a failure to behave with the level of care that someone of ordinary prudence would have exercised under the same circumstances."*

In the realm of Governance, Risk & Compliance (GRC), words have meaning and when you look at the meaning of *"level of care that someone of ordinary prudence"* that addresses the concept 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!

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 over 70% of FCA actions were initiated by whistleblowers who turned in their own company.
- 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 for negligence. While these insurance products are marketed as comprehensive protection from the full breadth of cyber-related risks, 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. After all, 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)[6] 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 Controlled Unclassified Information (CUI));
2. Defendant's breach of that duty (e.g., failure to protect CUI in accordance with DFARS requirements under NIST SP 800-171);
3. Plaintiff's sufferance 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 contractor 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 real property)

Determining A Breach Of Duty

When determining how whether the defendant has breached a duty, courts will usually use the *Learned Hand formula*, which is an algebraic approach to determining liability[7]. 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.

[6] *Cornell's Law School - https://www.law.cornell.edu/wex/negligence*
[7] *Learned Hand Formula - https://academic.oup.com/lpr/article/5/1/1/990799*