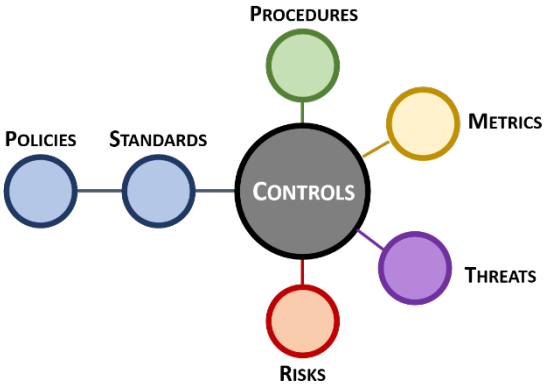
Integrated Controls Management (ICM) Overview

Version 2023.4

Table of Contents

EXECUTIVE SUMMARY

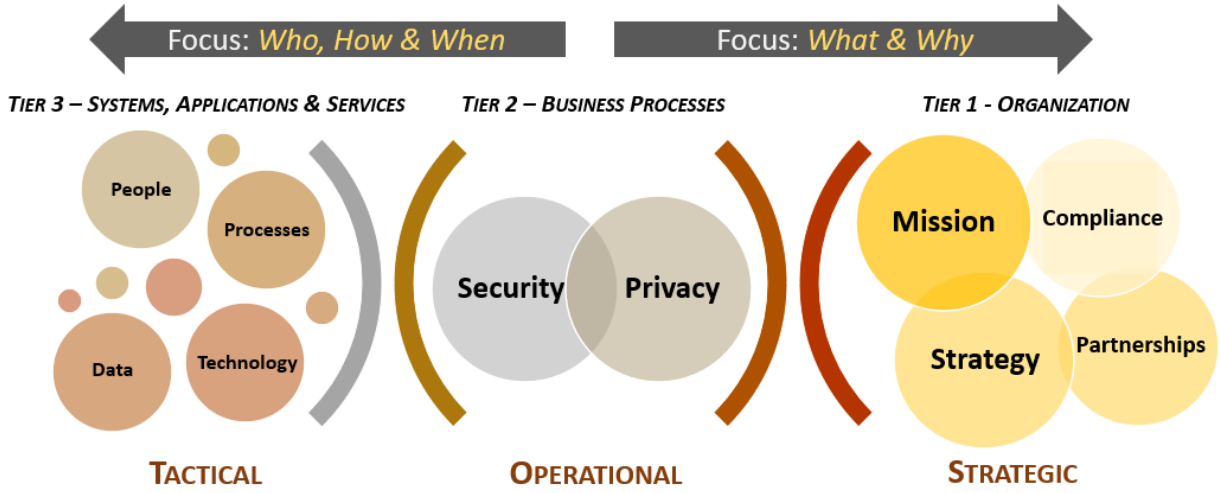
The premise of **Integrated Controls Management (ICM)** is that controls are central to cybersecurity & data privacy operations, as well as the overall business rhythm of an organization. This premise of the ICM is supported by the Security & Privacy Risk Management Model (**C|P-RMM**), that describes the central nature of controls, where not just policies and standards map to controls, but procedures, metrics, threats and risks, as well.



ICM takes a different approach from the traditional definition of Governance, Risk Management and Compliance (**GRC**) and/or Integrated Risk Management (**IRM**), since ICM is controls-centric, where controls are viewed as the nexus, or central pivoting point, for an organization's cybersecurity & data privacy operations.

OCEG defines GRC as, "*GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity,*" while Gartner jointly defines GRC/IRM as, "*a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.*" ComplianceForge and Secure Controls Framework (**SCF**), the developers of the ICM model, define ICM as, *"a holistic, technology-agnostic approach to cybersecurity & data privacy controls to identify, implement and manage secure and compliant practices, covering an organization's people, processes, technology and data, regardless of how or where data is stored, processed and/or transmitted."*

ICM is designed to proactively address the strategic, operational and tactical nature of operating an organization's cybersecurity & data privacy program at the control level. ICM is designed to address both internal controls, as well as the broader concept of Supply Chain Risk Management (SCRM).



Unlike GRC/IRM, ICM specifically focuses on the need to understand and clarify the difference between "compliant" versus "secure" since that is necessary to have coherent risk management discussions. To assist in this process, an organization's applicable controls are categorized according to "must have" vs "nice to have" requirements:

- Minimum Compliance Requirements (**MCR**) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, since they are merely compliance-related.
- Discretionary Security Requirements (**DSR**) are tied to the organization's risk appetite since DSR are "above and beyond" MCR, where the organization self-identifies additional cybersecurity & data privacy controls to address voluntary industry practices or internal requirements, such as findings from internal audits or risk assessments. DSR are primarily internally-influenced, based on the organization's respective industry and risk tolerance. While MCR establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

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

INTEGRATED CONTROLS MANAGEMENT (ICM)

ICM is defined as, *"a holistic, technology-agnostic approach to cybersecurity & data privacy controls to identify, implement and manage secure and compliant practices, covering an organization's people, processes, technology and data, regardless of how or where data is stored, processed and/or transmitted."*

In practical terms, controls exist to protect an organization's data. Requirements for asset management do not primarily exist to protect the inherent value of the asset, but the data it contains, since assets are merely data containers. Assets, such as laptops, servers and network infrastructure are commodities that can be easily replaced, but data residing on those devices cannot. This concept of being data-centric is crucial to understand when developing, implementing and governing a cybersecurity & data privacy program. ICM aides in that process.

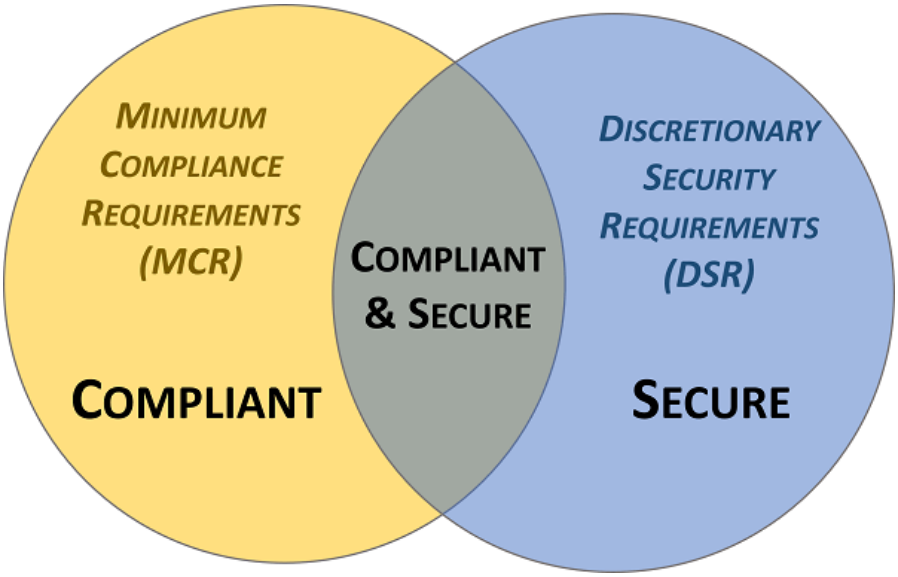
Similar in concept to Governance, Risk & Compliance (**GRC**) or Integrated Risk Management (**IRM**), ICM is focused on supporting processes and practices that must exist for a cybersecurity & data privacy program to operate effectively and efficiently. ICM is designed to proactively address the strategic, operational and tactical nature of operating an organization's cybersecurity & data privacy program.

DEFINING WHAT IT MEANS TO BE "SECURE & COMPLIANT"

Unlike GRC/IRM, ICM specifically focuses on the need to understand and clarify the difference between "compliant" versus "secure" since that is necessary to have coherent risk management discussions. To assist in this process, ICM helps an organization categorize its applicable controls according to "must have" vs "nice to have" requirements.

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

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



IT GENERAL CONTROLS (ITGC)

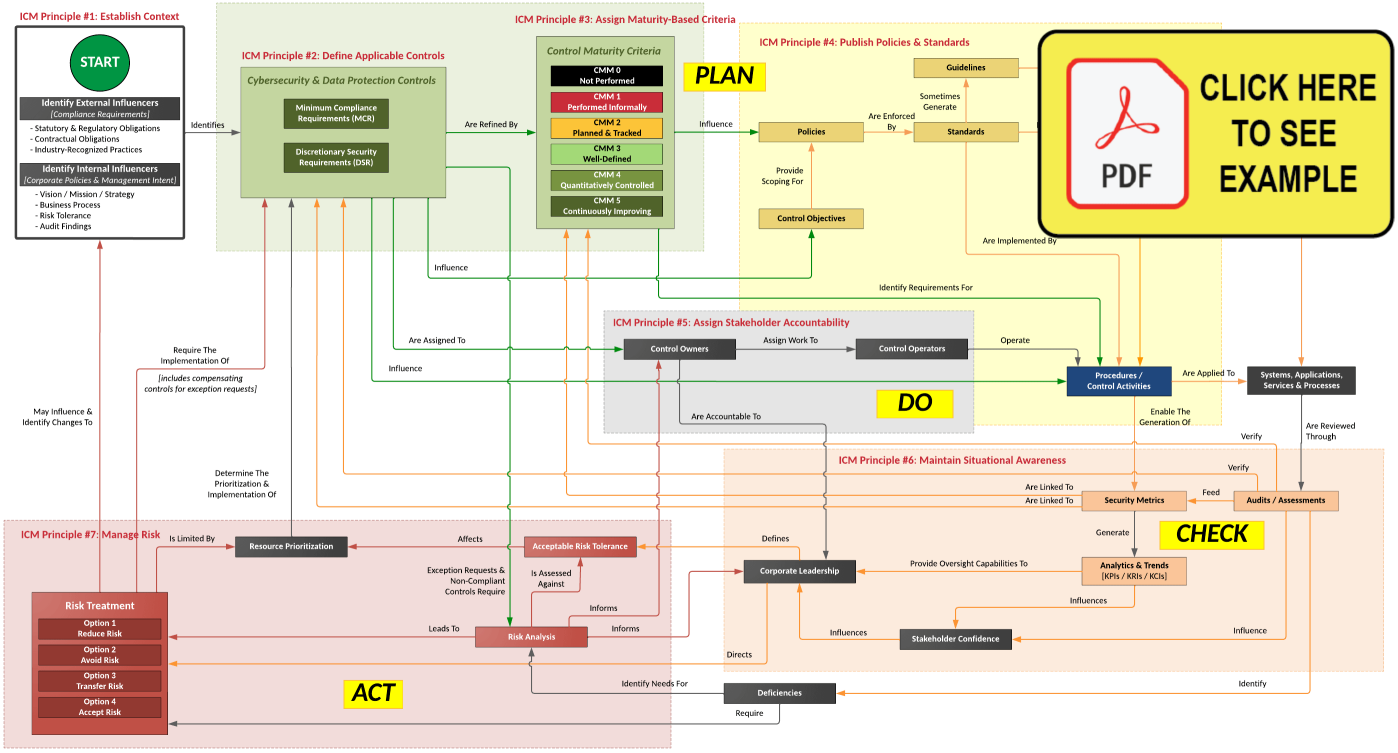
The combination of MCR and DSR equate to an organization's Minimum Security Requirements (**MSR**), which define the "must have" and "nice to have" requirements for People, Processes, Technology & Data (**PPTD**) in one control set. It defines the Minimum Viable Product (**MVP**) technical and business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

ICM Principles

There are eight (8) principles associated with ICM:

1. Establish Context
2. Define Applicable Controls
3. Assign Maturity-Based Criteria
4. Publish Policies, Standards & Procedures
5. Assign Stakeholder Accountability
6. Maintain Situational Awareness
7. Manage Risk
8. Evolve Processes

Integrated Controls Management (ICM) – Overlaid Onto The Integrated Cybersecurity Governance Model (ICGM)



[graphic can be downloaded from https://content.complianceforge.com/Plan-Do-Check-Act.pdf]

Principle 1: Establish Context

To build and maintain efficient and effective operations, a cybersecurity & data privacy program must have a hierarchical vision, mission and strategy that directly supports the organization's broader strategic objectives and business processes. This process of establishing context involves identifying all applicable external compliance requirements (e.g., laws, regulations and contractual obligations), as well as internal directives (e.g., Board of Directors, corporate policies, etc.). This is a due diligence element of the cybersecurity & data privacy program.

Principle 2: Define Applicable Controls

A tailored control set cybersecurity & data privacy controls must exist. This control set needs to be made of Minimum Compliance Requirements (**MCR**) and Discretionary Security Requirements (**DSR**). This blend of "must have" and "nice to have" requirements establish an organization's tailored control set to ensure both secure practices and compliance.

Principle 3: Assign Maturity-Based Criteria

The cybersecurity & data privacy program must assign maturity targets to define organization-specific "what right looks like" for controls. This establishes attainable criteria for people, processes and technology requirements. Tailored maturity level criteria can be used to plan for, budget for and assess against. Maturity targets should support the organization's need for operational resiliency.

PRINCIPLE 4: PUBLISH POLICIES & STANDARDS

Documentation must exist, otherwise an organization's cybersecurity & data privacy practices are unenforceable. Formalizing organization-specific requirements via policies and standards are necessary to operationalize controls. Documented policies and standards provide evidence of due diligence that the organization identified and implemented reasonable steps to address its applicable requirements.

PRINCIPLE 5: ASSIGN STAKEHOLDER ACCOUNTABILITY

Controls must be assigned to stakeholders to ensure accountability (e.g., business units, teams and/or individuals). These "control owners" may assign the task of executing controls to "control operators" at the Individual Contributors (**IC**)-level. Stakeholders utilize the prescriptive requirements from policies and standards to develop Standardized Operating Procedures (**SOP**) that enable ICs to execute those controls. The documented execution of procedures provides evidence of due care that reasonable practices are being performed.

PRINCIPLE 6: MAINTAIN SITUATIONAL AWARENESS

Situational awareness must involve more than merely "monitoring controls" (e.g., metrics). While metrics are a point-in-time snapshot into discrete controls' performance, the broader view of metrics leads to a longer-term trend analysis. When properly tied in with current risk, threat and vulnerability information, this insight provides "situational awareness" that is necessary for organizational leadership to adjust plans to operate within the organization's risk threshold.

PRINCIPLE 7: MANAGE RISK

Proactive risk management processes must exist across all phases of development/information/system life cycles to address confidentiality, integrity, availability and safety aspects. Risk management must address internal and external factors, including privacy and Supply Chain Risk Management (**SCRM**) considerations. To manage risk, it requires the organization to enforce a clearly defined risk threshold and ensure reasonable security practices are operational.

PRINCIPLE 8: EVOLVE PROCESSES

Cybersecurity & data privacy measures must adapt and evolve to address business operations and the evolving threat landscape. This requires the adoption of a Plan, Do, Check & Act (**PDCA**) approach (e.g., Deming Cycle) to ensure the organization proactively identifies its requirements, implements appropriate protections, maintains situational awareness to detect incidents, operates a viable capability to respond to incidents and can sustain key business operations, if an incident occurs.

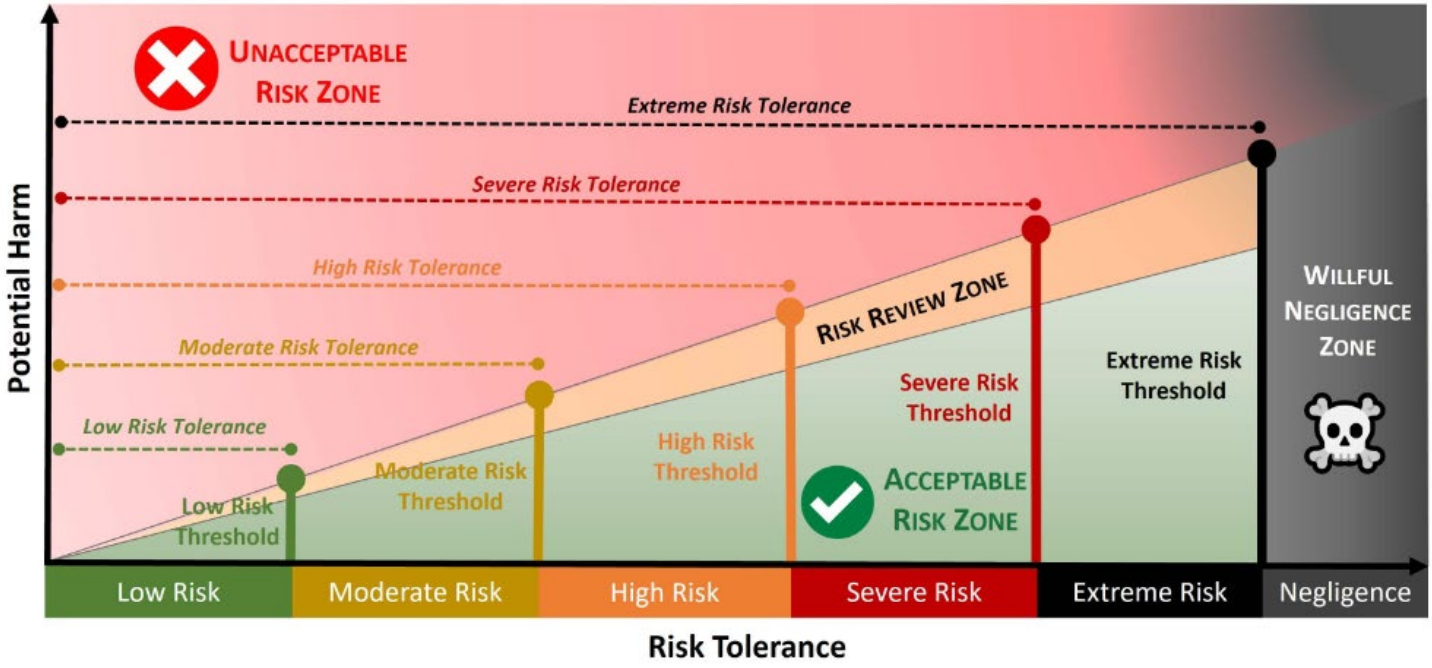
PRACTICAL RISK MANAGEMENT CONSIDERATIONS

Controls are the nexus of a cybersecurity & data privacy program, so it is vitally important to understand how controls should be viewed from a high-level risk management perspective. To progress from identifying a necessary control to a determination of risk, it is a journey that has several steps, each with its own unique terminology. Therefore, it is important to baseline the understanding risk management terminology.

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.



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.

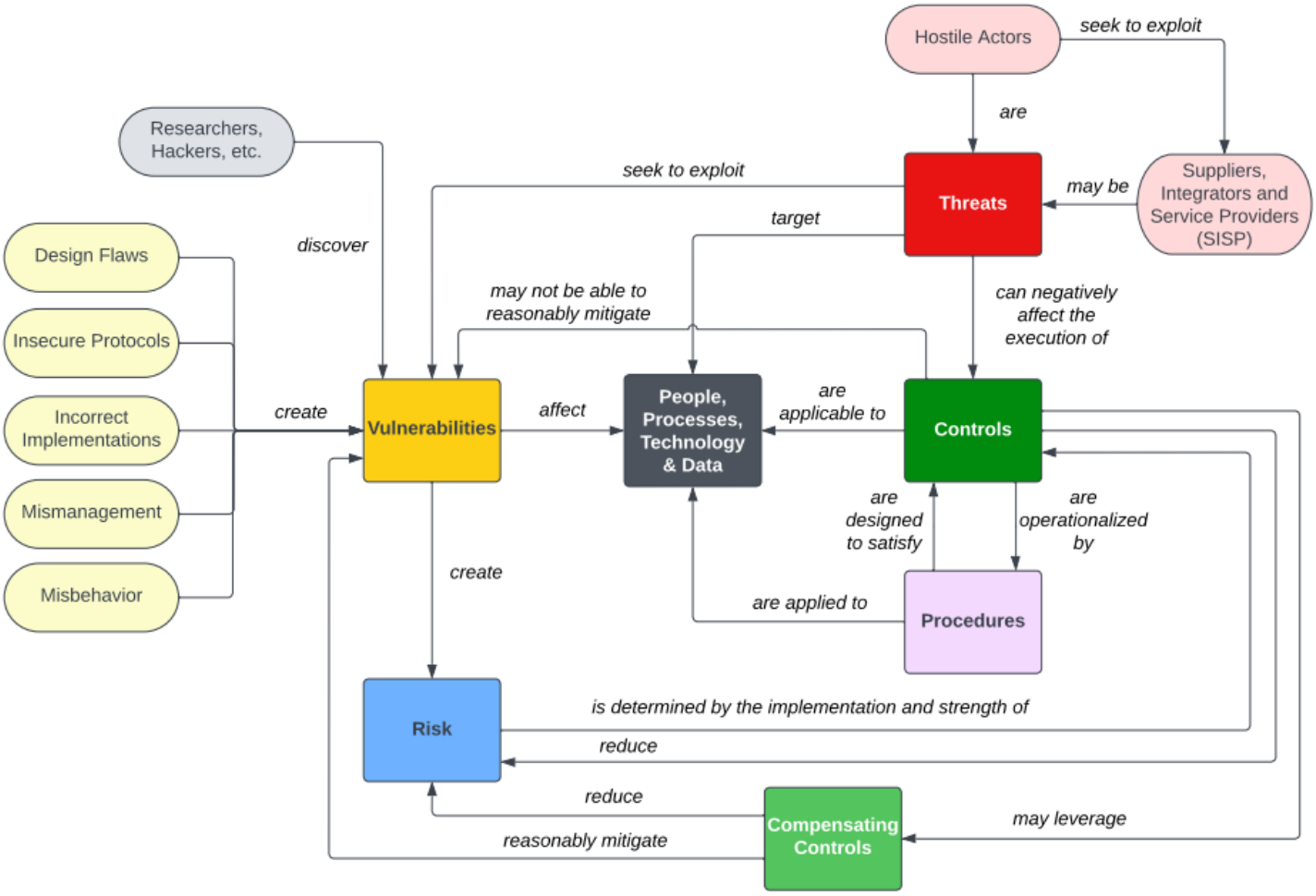
RISK MANAGEMENT OPTIONS

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

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

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

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 cybersecurity & data privacy practices, "risk" is defined as:

- noun *A situation where someone or something valued is exposed to danger, harm or loss.*
- verb *To expose someone or something valued to danger, harm or loss.*

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

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

The intent of standardizing risk terminology for categories is so that all the organization's personnel can speak the same "risk language" across the enterprise. Categorization also allows management to compare and prioritize risks.

What Is A Threat?

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

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

[1] *Risk vs Threat vs Vulnerability Ecosystem - https://content.complianceforge.com/Risk-Threat-Vulnerability-Ecosystem.pdf*

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

According to the Project Management Body of Knowledge (**PMBOK®**) Guide:[2]

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

A risk appetite does not contain granular risk management criteria and is primarily a "management statement" that is subjective in nature. Similar in concept to how a policy is a *"high-level statement of management intent,"* an organization's defined risk appetite is a high-level statement of how all, or certain types of, risk are willing to be accepted. [3]

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 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.

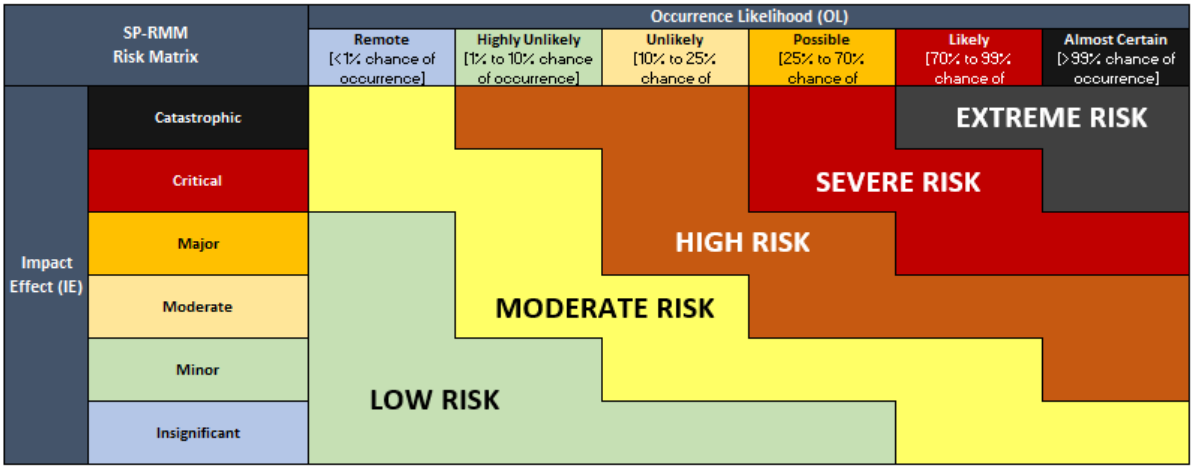
There are two (2) objective criteria that go into defining what constitutes a low, moderate, high, severe or Extreme Risk includes:

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

---

[2] *PMBOK® Guide - https://www.pmi.org/pmbok-guide-standards/foundational/pmbok*

[3] *ComplianceForge Hierarchical Cybersecurity Governance Framework (HCGF) - https://content.complianceforge.com/Hierarchical-Cybersecurity-Governance-Framework.pdf*



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 (**MSSP**s), etc.)
- Manufacturing (high value)
- Healthcare
- Defense Industrial Base (**DIB**) contractors and subcontractors
- Legal services (e.g., law firms)
- Construction (high value)

High Risk Tolerance

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

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

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

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

Severe Risk Tolerance

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

- Are in an unregulated industry, pertaining to cybersecurity and/or data privacy requirements.
- Do not store, process and/or transmit sensitive/regulated data.

- Lack management support for cybersecurity and data privacy governance practices.
- Do not have cyber-related liability insurance.

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

- Startups
- Artificial Intelligence (**AI**) developers

EXTREME RISK TOLERANCE

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

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

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

- Startups
- Artificial Intelligence (**AI**) developers

WHAT IS A RISK THRESHOLD?

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

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

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

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

DEFINING A RISK DETERMINATION

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

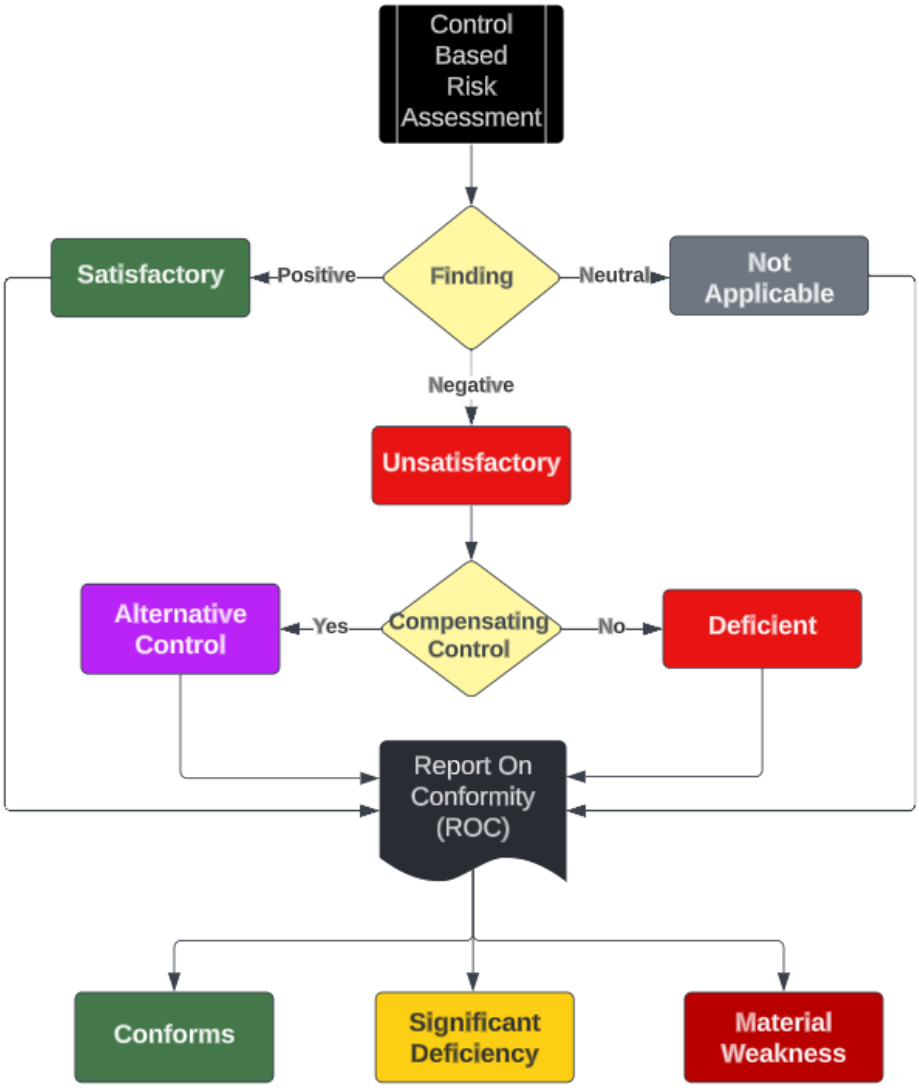
When an organization goes through some form of "certification" process, it undergoes a conformity assessment (e.g., ISO 27001, CMMC, SOC 2, PCI DSS, RMF, etc.). Conformity assessments are designed to assure that a particular product, service, or system meets a given level of quality or safety. Instead 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. Alternative 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 three (3) following risk determinations:

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



CONFORMS

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

At the control level, there may be one or more deficient controls, but as a whole, the cybersecurity and data privacy practices support the organization's stated risk tolerance.

A statement that the assessed controls conform 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.

SIGNIFICANT DEFICIENCY

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

This indicates cybersecurity and data privacy practices fail to support the organization's stated risk tolerance. This is less severe than a

material weakness, but merits executive leadership attention.

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.

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

Material Weakness

This is a negative outcome and indicates the organization is unable to demonstrate conformity with its selected cybersecurity and data privacy practices, due to deficiencies that make it probable that reasonable 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.

This indicates cybersecurity and data privacy practices fail to support the organization's stated risk tolerance.

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."*[4]

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:

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

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

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."*[5]
- 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."*[6]

[4] *SCF Cybersecurity Materiality - https://securecontrolsframework.com/cybersecurity-materiality/*
[5] *SEC - https://www.sec.gov/comments/265-24/26524-77.pdf*
[6] *IFRS - https://www.ifrs.org/content/dam/ifrs/project/definition-of-materiality/definition-of-material-feedback-statement.pdf*

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.

APPLYING ICM TO GOVERNANCE, RISK MANAGEMENT & COMPLIANCE (GRC) FUNCTIONS

GRC can be a costly and labor-intensive endeavor, so what justifies the investment? Essentially, GRC functions help avoid negligence, with the added benefit of improved IT/cyber/privacy operating effectiveness. The reality of the situation is your company invests in cybersecurity & data privacy as a necessity. This necessity is driven in large part by laws, regulations and contractual requirements that it is legally obligated to comply with. It is also driven by the desire to protect its public image from damaging acts that happen when cybersecurity & data privacy practices are ignored. Regardless of the specific reason, those charged with developing, implementing and running your organization's cybersecurity & data privacy program must do so in a reasonable manner that would withstand scrutiny that could take the form of an external auditor, regulator or prosecuting attorney.

How fast would you drive your car if you didn't have any brakes? Think about that for a moment - you would likely drive at a crawl in first gear and even then you would invariably have accidents as you bump into objects and other vehicles to slow down. Brakes on a vehicle actually allow you to drive fast, in addition to safely navigating dangers on the road!

While it is not the most flattering analogy, GRC is akin to the brakes on your car, where they enable a business' operations to go fast and avoid catastrophic accidents. Without those "brakes", an accident is a certainty! These brakes that enable a business' operations to stay within the guardrails are its cybersecurity policies, standards and procedures. These requirements constitute "reasonable practices" that the organization is required to implement and maintain to avoid being negligent.

GRC IS A PLAN, DO, CHECK & ACT (PDCA) ADVENTURE – THAT IS A CONCEPT THAT SHOULD BE EMBRACED, NOT FOUGHT AGAINST

GRC most often deals with legally-binding requirements, so it is important to understand that negligence is situationally-dependent. For example, an intoxicated driver who gets behind the wheel acting negligently. However, when sober, that same individual is a champion race car driver who is highly skilled and would not be considered incompetent in any regard. In this example, driving intoxicated constitutes a negligent act and shows that negligence has nothing to do with being incompetent. The point is to demonstrate that an organization can employ many highly-competent personnel, but even competent people can behave in a negligent manner. GRC fundamentally exists to help an organization avoid circumstances that could be construed as negligent acts.

Considering how business practices continuously evolve, so must cybersecurity practices. The Plan, Do, Check & Act (**PDCA**) process (also referred to as the Deming Cycle) enables the GRC function to continuously evaluate risks, threats and performance trends, so that the organization's leadership can take the necessary steps to minimize risk by modifying how people, processes and technology work together to keep everything both secure and operational. The PDCA approach is a logical way to conceptualize how GRC works:

- **Plan**. The overall process beings with planning. At its core, this phase is the process of conducting due diligence. The results of this process will define necessary controls (e.g., requirements) that influence the need for policies, standards and procedures. These actions directly influence resourcing and procurement actions that range from staffing needs to tool purchases and services acquisition.
- **Do**. This phase is the process of conducting due care, where it is focused on the "reasonable care" necessary to properly and sufficiently conduct operations that demonstrate the absence of negligence. This is the execution of procedures – the processes that bring controls to life.
- **Check** This phase can be considered maintaining situational awareness. There are several ways to maintain situation awareness and that ranges from control validation testing to audits/assessments and metrics.
- **Act**- This phase again brings up the concept of "reasonable care" that necessitates taking action to maintain the organization's targeted risk tolerance threshold. This deals with addressing two main concepts (1) real deficiencies that currently exist and (2) areas of concern that may expose the organization to a threat if no action is taken.

The premise is that controls are central to cybersecurity & data privacy operations as well as the business rhythms of the organization. Without properly defining MCR and DSR thresholds, an organization's overall cybersecurity & data privacy program is placed in jeopardy as the baseline practices are not anchored to clear requirements. Furthermore, understanding and clarifying the difference between "compliant" versus "secure" (e.g., MCR vs. MCR+DSR) enhances risk management discussions.

CHICKEN VS EGG DEBATE: THE LOGICAL ORDER OF GRC FUNCTIONS

Which comes first? Governance, Risk or Compliance? This has been a hotly-debated topic since GRC was first coined nearly 20 years ago. There is a logical order to GRC processes that must be understood to avoid siloes and an improperly scoped security program. First, it is necessary to level-set on the terminology of what GRC functions do:

- Governance. Structures the organization's controls to align with business goals and applicable statutory, regulatory, contractual and other obligations. Develops necessary policies and standards to ensure the proper implementation of controls.
- Risk Management. Identifies, quantifies and manages risk to information and technology assets, based on the organization's operating model.
- Compliance. Oversight of control implementation to ensure the organization's applicable statutory, regulatory, contractual and other obligations are adequately met. Conducts control validation testing and audits/assessments.

When establishing GRC practices, what is described below is the precedence of how (1) compliance influences (2) governance, which influences (3) risk management. This addresses the "GRC chicken vs egg" debate:

COMPLIANCE

The genesis of GRC is to first identify applicable statutory, regulatory and contractual obligations that the organization must adhere to, as well as internal business requirements (e.g., Board of Director directives). This is a compliance function that identifies statutory, regulatory and contractual obligations. It is a due diligence exercise to identify what the organization is reasonably required to comply with from a cybersecurity & data privacy perspective. This process involves interfacing with various Lines of Business (**LOB**) to understand how the organization operates, including geographic considerations. Generally, Compliance needs to work with the legal department, contracts management, physical security and other teams to gain a comprehensive understanding of the organizational compliance needs.

Compliance is the "source of truth" for statutory, regulatory and contractual obligations. With that knowledge, Compliance informs Governance about the controls that apply to applicable laws, regulations and frameworks. This knowledge is needed so that Governance can determine the appropriate policies and standards that must exist. Compliance may identify requirements to adhere to a specific industry framework (e.g., NIST CSF, ISO 27002, NIST 800-53, etc.), but organizations are usually able to pick the framework that best fits their needs on their own. This is often where various compliance obligations exceed what a single framework can address, so the organization must leverage some form of metaframework (e.g., framework of frameworks).

Compliance defines the controls necessary to meet the organization's specific needs (e.g., MCR + DSR) and publishes one or more control sets (e.g., specific to a project/contract/law/regulation or organization-wide controls). The control set(s) can be considered an organization's Minimum Security Requirements (**MSR**) that will be used:

- By the Governance team to develop appropriate policies, standards and other information (e.g., program-level guidance, CONOPS documents, etc.; and
- By the Risk Management team to assess risk.

Since not all controls are weighted equally, it is vitally important that personnel who represent the Risk Management function are involved in developing an assigned weight for each control (e.g., the presence of a fully-patched border firewall should be considered a more important control than end user awareness posters). This weighting of cybersecurity & data privacy controls is necessary to ensure the results of risk assessments accurate support the intent of the organization's risk tolerance threshold. That threshold is meant to establish a benchmark for defining acceptable and unacceptable risk.

GOVERNANCE

Based on these controls, Governance has a few key functions:

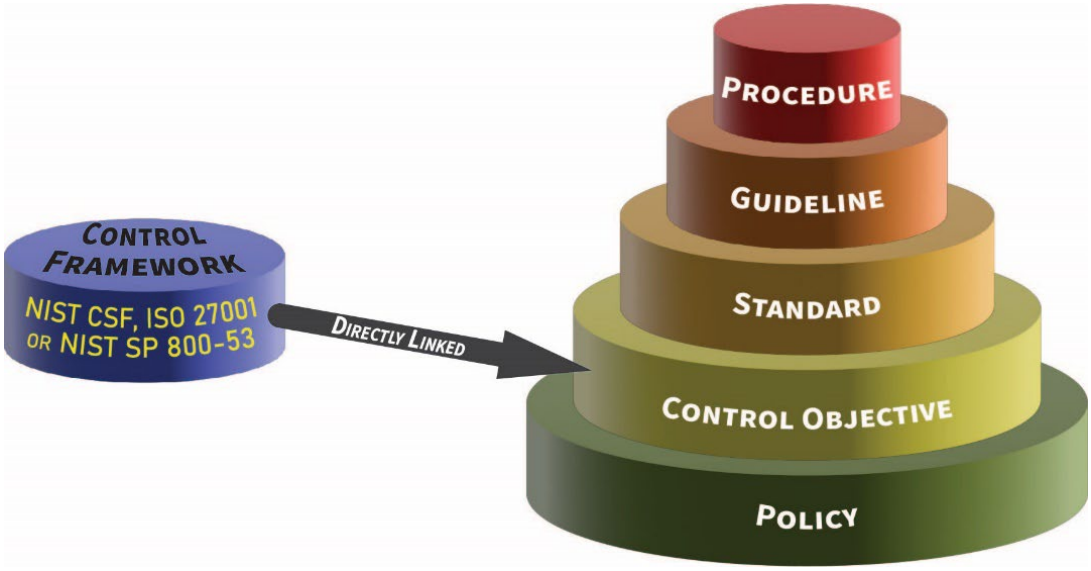
- Develop policies and standards to meet those compliance obligations (defined by applicable control objectives); and
- Assign ownership of those controls to the applicable stakeholders involved in the affected business processes. This process often requires a documented Responsibility, Accountability, Supportive, Consulted and Informed **(RASCI)** chart to ensure the organizational model supports effective implementation and oversight of the assigned controls.

Personnel representing the Governance function must work directly with the stakeholders (e.g., control owners and control operators) who are directly responsible for implementing and operating their assigned cybersecurity & data privacy controls. Those stakeholders are expected to develop and operate Standardized Operating Procedures (**SOP**) to ensure control implementation is performed according to the company's performance requirements, as established in the organization's cybersecurity & data privacy standards. The operation of those SOPs generates evidence of due care that reasonable practices are in place and operating accordingly. Generating deliverables is an expected output from executing procedures.

The development and implementation of the policies and standards is evidence of due diligence that the organization's compliance obligations are designed to address applicable administrative, technical and physical security controls. It is important to ensure that policies and standards document what the organization is doing, as the policies and standards are often the mechanisms by which outside regulators measure implementation and maturity of the control. Organizational governance can be a vital element in the organizations ability to implement, sustain and defend their compliance program.

Cybersecurity & data privacy documentation is generally comprised of six (6) main parts:

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



RISK MANAGEMENT

From a trickle-down perspective, while Risk Management logically follows both Compliance and Governance functions in establishing a GRC program, Risk Management is crucial for the organization to maintain situational awareness and remain both secure and compliant. Risk Management serves as the primary "canary in the coal mine" to identify instances of non-compliance that lead to the improper management of risks and exposure of the organization to threats; since ongoing risk assessments generally occur more frequently than internal/external audits that Compliance may oversee.

Risk Management activities addresses both due diligence and due care obligations to identify, assess and remediate control deficiencies:

- Risk Management must align with Governance practices for exception management (e.g., compensating controls).
- Compliance must evaluate findings from risk assessments and audits/assessments (both internal and external) to determine if adjustments to the organization's cybersecurity & data privacy controls (e.g., MCR + DSR) are necessary, based on business process changes, technology advancements and/or an evolution of the organization's risk threshold.

While Risk Management personnel do not perform the actual remediation actions (that is the responsibility of the control owner), Risk Management assists in determining the appropriate risk treatment options:

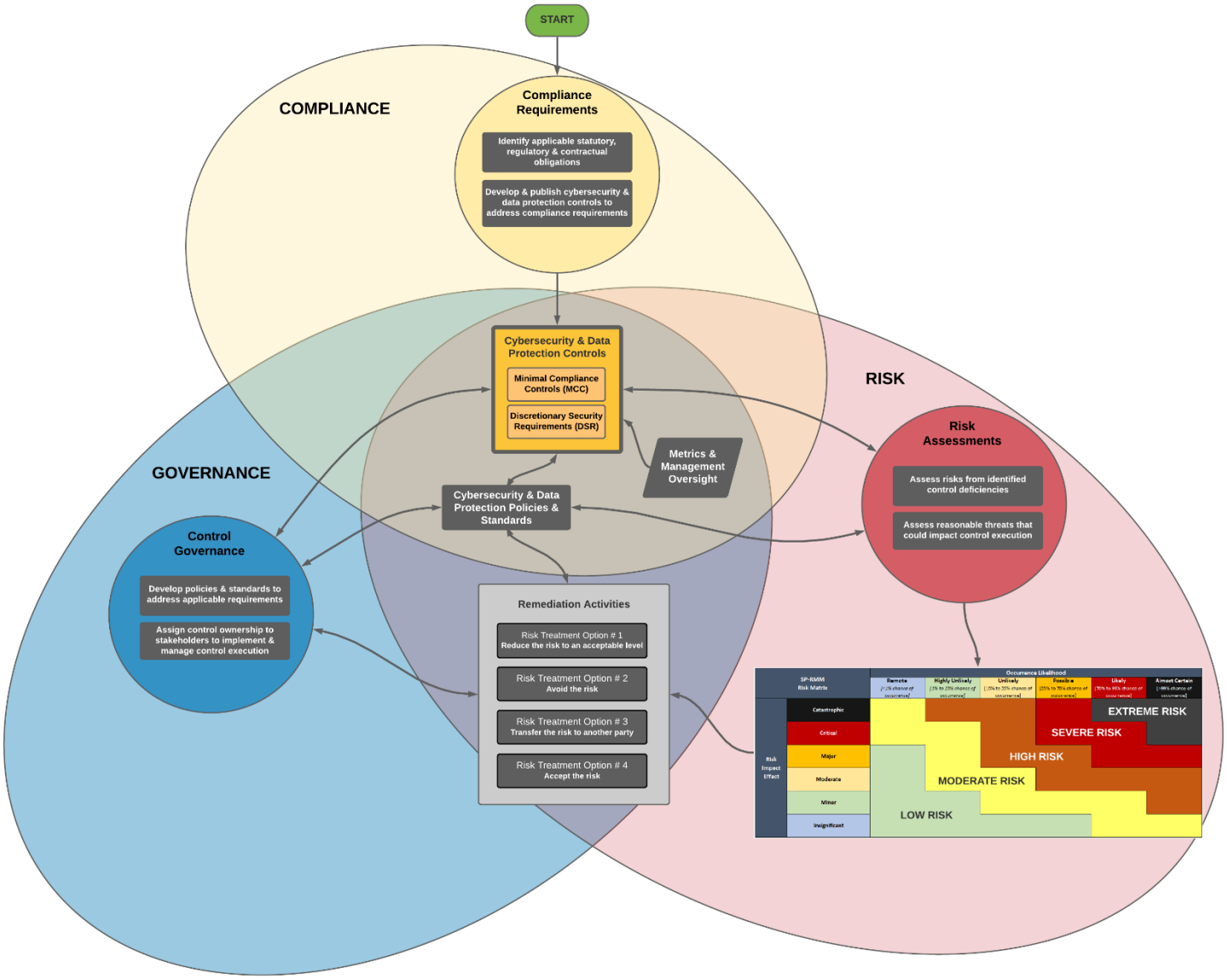
- Reduce the risk to an acceptable level;
- Avoid the risk;
- Transfer the risk to another party; or
- Accept the risk.

One key consideration for GRC, especially Risk Management, is that the appropriate level of organizational management makes the risk management decision. Therefore, risks need to be ranked, so that the appropriate levels of management can be designated as "approved authorities" to make a risk treatment determination. For example, a project manager should not be able to accept a "high risk" that

should be made by a VP or some other executive. By formally-assigning risk to individuals and requiring those in managerial roles to own their risk management decisions, it can help the organization maintain its target risk threshold.

GRC Integrations

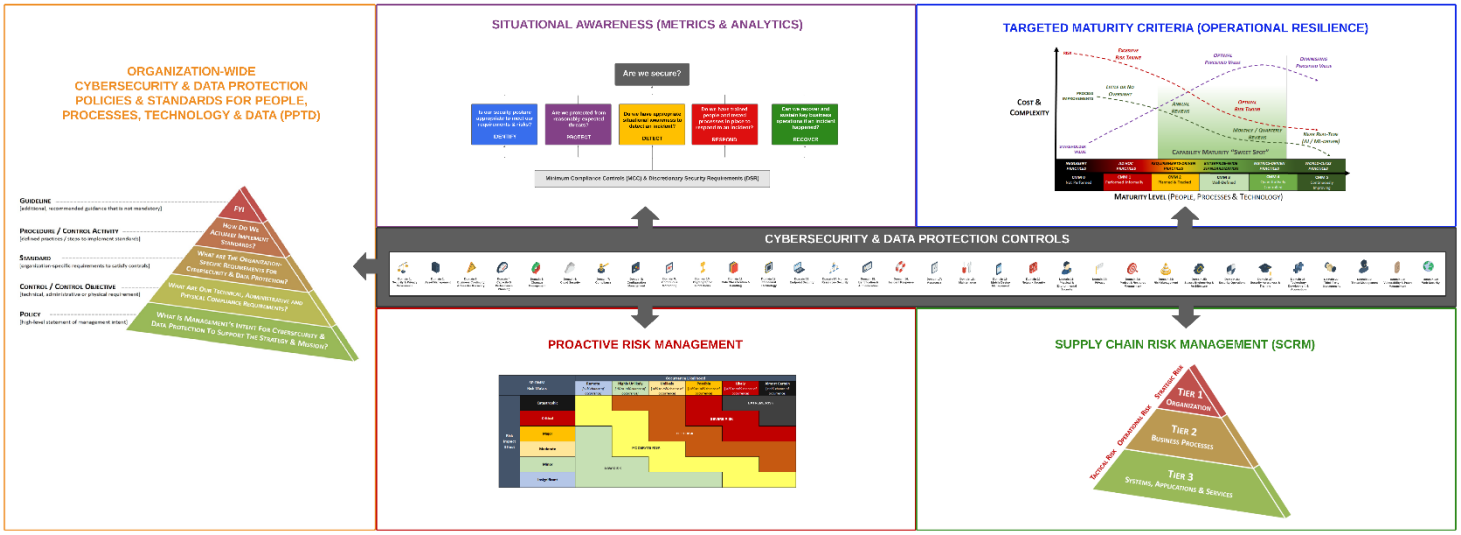
The processes described above can be visualized in the following diagram which shows the interrelated nature of governance, risk management and compliance functions to build and maintain an organization's cybersecurity & data privacy program.



[graphic can be downloaded from https://content.complianceforge.com/ICM-GRC.pdf]

PRACTICAL SOLUTIONS TO IMPLEMENT ICM

ICM is meant to be put into practice by organizations of any size or industry. The information below provides an understanding of available options to implement ICM with existing solutions.



[graphic can be downloaded from https://content.complianceforge.com/ICM-Principles.pdf]

CYBERSECURITY & DATA PROTECTION CONTROLS

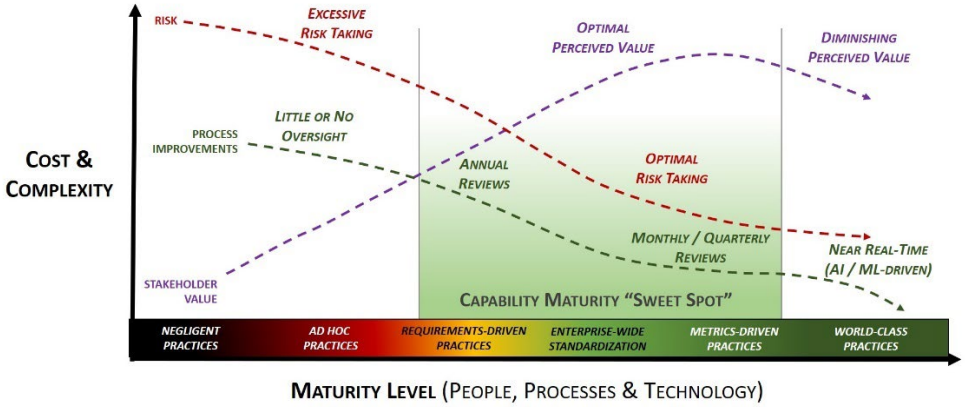
While it is possible to use any control set, ICM was specifically designed based on the comprehensive nature of the Secure Controls Framework (**SCF**). The SCF has thirty-two (32) domains that address cybersecurity & data privacy-related requirements. The SCF is licensed according to Creative Commons, so it is free for organizations to use. The SCF contains:

- Cybersecurity & data privacy-related controls that are organized by domain;
- Weighting;
- Maturity model criteria;
- Risk catalog;
- Threat catalog; and
- Controls written in question format to aid in performing control assessments.

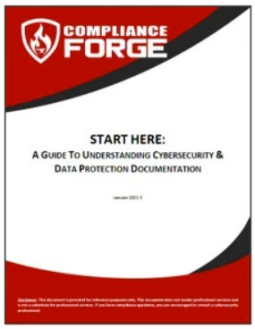
MATURITY-BASED CONTROL CRITERIA

The SCF contains the Cybersecurity & Data Privacy Capability Maturity Model (**C|P-CMM**) that provides maturity model criteria definitions for each SCF control.

- The C|P-CMM is based on the Systems Security Engineering Capability Maturity Model (**SSE-CMM**); and
- Each SCF control has entries for CMM level 0 through level 5 pre-populated to provide maturity-based guidance on controls.



Documented Policies, Standards & Procedures



There are generally three options to obtaining cybersecurity & data privacy documentation:

1. Use internal resources to write it in-house;
2. Hire a consultant to write a bespoke set of documentation; or
3. Purchase semi-customized templates online.

ComplianceForge wrote a guidebook to help organizations understand cybersecurity & data privacy documentation. This guide is a free resource to educate organizations on "what right looks like" for documentation, based on definitions from authoritative sources.

Assign Stakeholder Accountability

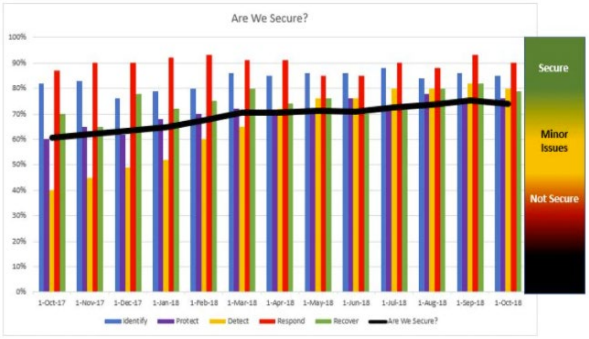
Assigning stakeholder accountability offers unique challenges for organizations, since it is beyond cybersecurity & data privacy that involves Human Resources (**HR**), procurement and sometimes legal teams to ensure accountability is enforceable.

The best starting point is the NIST SP 800-181, *Workforce Framework for Cybersecurity (NICE Framework)*.[7] The NICE Framework offers an efficient way to assign stakeholder accountability for internal and external stakeholders.

Maintain Situational Awareness

Maintaining situational awareness has different meanings, based on the security culture of an organization. For some organizations, it means metrics, while for others it means a broader understanding of control performance, risks, threats and current vulnerability information.

The ComplianceForge Security Metrics Reporting Model™ (**SMRM**) takes a practical view towards implementing a sustainable metrics reporting capability. At the end of the day, executive management (e.g., CIO, CEO, Board of Directors (BoD), etc.) often just want a simple answer to a relatively-straightforward question: "Are we secure?" In order for a CISO to honestly provide an answer, it requires a way for the CISO to measure and quantify an "apples and oranges" landscape where processes and technologies lack both uniform risk weighting and abilities to capture metrics. The SMRM helps solve this aspect of dissimilarity by utilizing a weighted approach to metrics that generate Key Performance Indexes (**KPXs**) as a way to logically-organize and report individual metrics. Using KPX enables the SMRM to provide a reasonable and defendable answer.

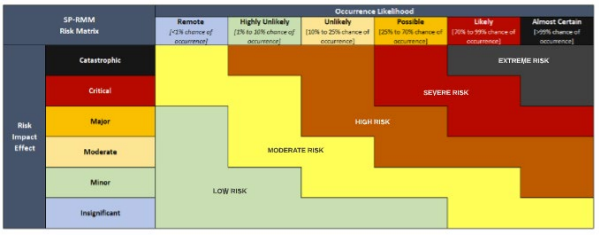


Manage Risk

The SCF contains the Cybersecurity & Data Privacy Risk Management Model (**C|P-RMM**) that provides a control-centric:

- Risk catalog;
- Threat catalog; and
- Methodology to perform a risk assessment.

The value of the C|P-RMM is having a standardized methodology where controls are tied to specific risks and threats. Based on the other criteria offered by the SCF (e.g., weighting and maturity criteria), the C|P-RMM makes calculating risk a straightforward process.

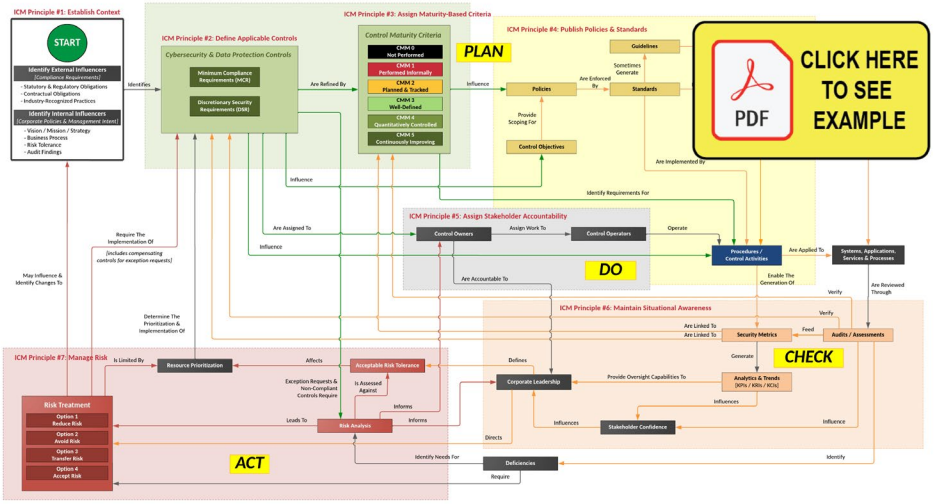


[7] NIST SP 800-181 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

EVOLVE PROCESSES

The ICM utilizes a Plan, Do, Check & Act (**PDCA**) approach that is a logical way to design a governance structure:

- Plan. The overall ICM process beings with planning. This planning will define the policies, standards and controls for the organization. It will also directly influence the tools and services that an organization purchases, since technology purchases should address needs that are defined by policies and standards.
- Do. Arguably, this is the most important section for cybersecurity & data privacy practitioners. Controls are the "security glue" that make processes, applications, systems and services secure. Procedures (also referred to as control activities) are the processes how the controls are actually implemented and performed.
- Check. In simple terms, this is situational awareness. Situational awareness is only achieved through reporting through metrics and reviewing the results of audits/assessments.
- Act. This is essentially risk management, which is an encompassing area that deals with addressing two main concepts (1) real deficiencies that currently exist and (2) possible threats to the organization.



[graphic can be downloaded from https://content.complianceforge.com/Plan-Do-Check-Act.pdf]