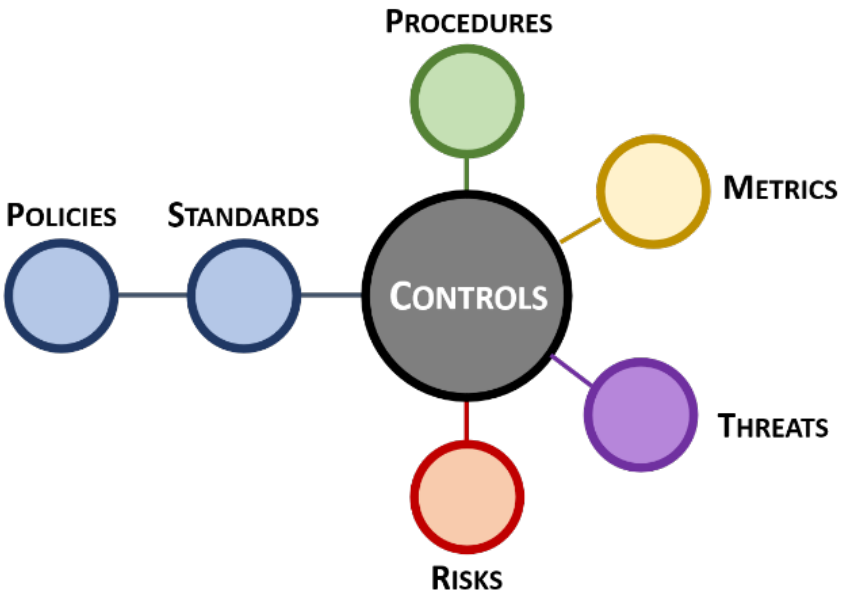
Integrated Controls Management (ICM) Overview



Version 2024.3

Table of Contents

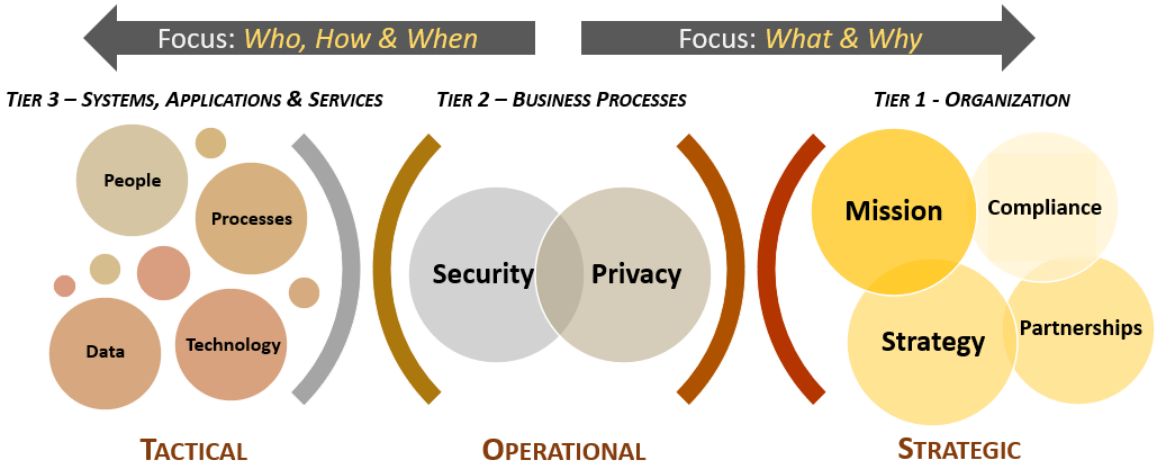
EXECUTIVE SUMMARY

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 Cybersecurity & Data Privacy Risk Management Model (**C|P-RMM**),[1] 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).



Secure and compliant operations exist when applicable controls are properly scoped and implemented. 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.

[1] SCF C|P-RMM - https://securecontrolsframework.com/risk-management-model/

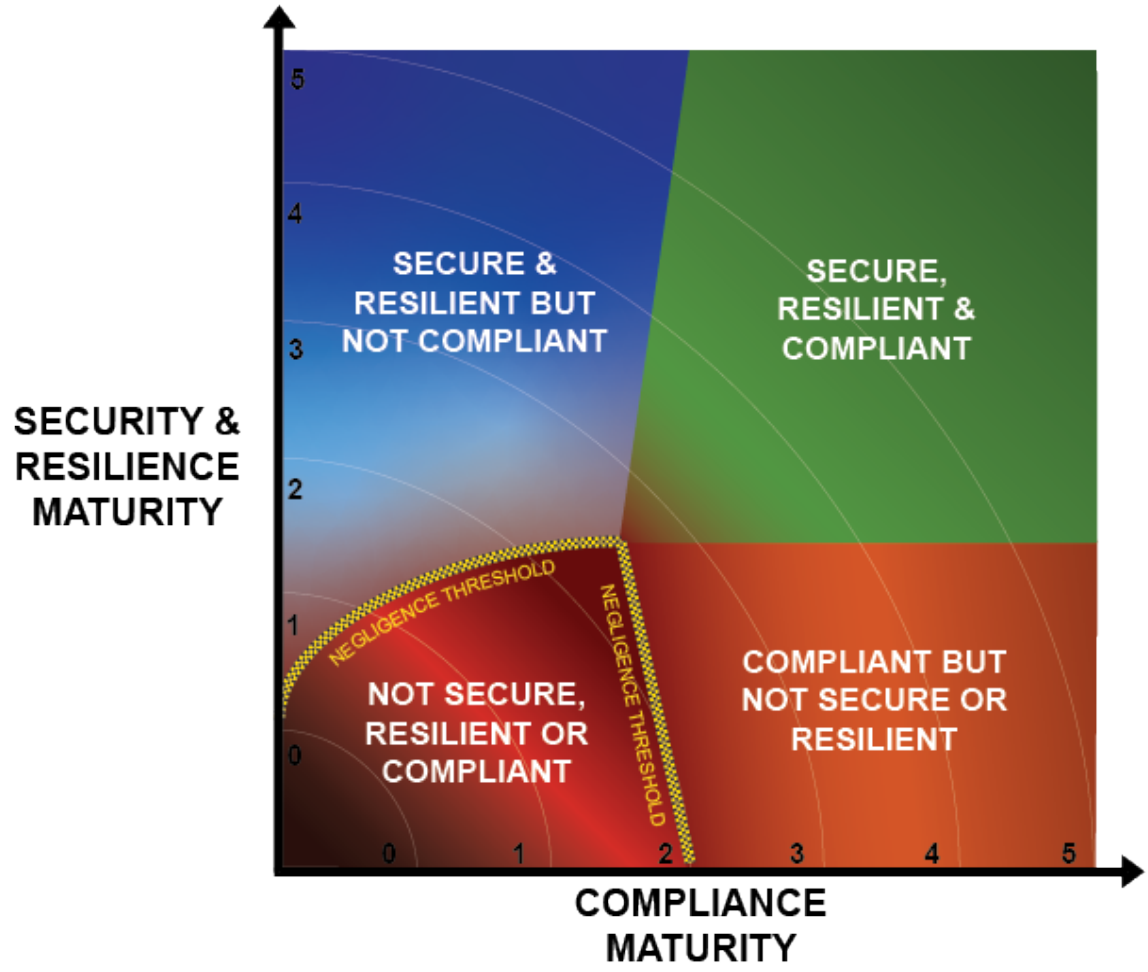
SECURITY VS COMPLIANCE

For those on the receiving end of cybersecurity efforts, the terms "security" and "compliance" might seem synonymous. However, understanding the subtle, yet crucial, differences between being compliant and being secure is paramount in safeguarding an organization's technologies and sensitive/regulated data.

There is a long-running debate pertaining to "compliance is not security" and there is some truth to that saying. However, instead of a binary state of being compliant versus secure, it should be viewed as four (4) maturity-based quadrants where your organization is either:

1. Not secure, resilient or compliant (negligent);
2. Secure & resilient, but not compliant;
3. Compliant, but not secure or resilient; or
4. Secure, resilient & compliant.

The underlying issue in the "compliance vs security" debate is complacency and this is important for the broader concept of Integrated Controls Management (**ICM**). Your adversaries are unrelenting, so why would you consciously choose to settle? That is where the concept of negligence comes into play, when your failure to conduct due diligence and due care activities can be considered negligent behavior. That term tends to scare executives, and it should, but it does not change the reality that there is a negligence threshold that is specific to each organization. The question for you is, *"Do you know what your negligence threshold is, based on your applicable laws, regulations and contractual obligations?"*



This concept of identifying a negligence threshold is addressed in the SCF's Cybersecurity & Data Privacy Capability Maturity Model (**C|P-CMM**).[2]

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

Defining Compliance That Is Specific To Your Business Case

Compliance controls are viewed as "must have" requirements that are non-discretionary (e.g., not optional). These requirements directly sourced from an organization's applicable laws, regulations and contractual obligations. From a scoping perspective, these compliance obligations may be organization-wide or narrowly scoped to a specific enclave or project. It is your organization's responsibility to properly scope the applicability of these compliance controls. The Unified Scoping Guide (**USG**) is an excellent resource for your scoping exercise.[3]

The process of clearly identifying non-discretionary controls generally involves interviewing multiple stakeholders to gain appropriate situational awareness of all pertinent compliance obligations. These stakeholders with valuable insights are often:

- Procurement / Contracts Management;
- Enterprise Risk Management (**ERM**);
- Legal;
- Physical Security; and
- Human Resources.

Statutory Obligations

Statutory obligations are required by law and refer to current laws that were passed by a state or federal government. From a cybersecurity and data privacy perspective, statutory compliance requirements includes state, Federal and international laws:

- Fair and Accurate Credit Transactions Act (**FACTA**)
- Family Education Rights and Privacy Act (**FERPA**)
- Federal Information Security Management Act (**FISMA**)
- Federal Trade Commission (**FTC**) Act
- Gramm-Leach-Bliley Act (**GLBA**)
- Health Insurance Portability and Accountability Act (**HIPAA**)
- Sarbanes-Oxley Act (**SOX**)
- California - SB 1386 / CCPA / CPRA
- Massachusetts - 201 CMR 17.00
- Oregon - ORS 646A.622
- Canada - Personal Information Protection and Electronic Documents Act (**PIPEDA**)
- UK - Data Protection Act (**DPA**)

Regulatory Obligations

Regulatory obligations are required by law, but are different from statutory requirements in that these requirements refer to rules issued by a regulating body that is appointed by a state or federal government. These are legal requirements through proxy, where the regulating body is the source of the requirement. It is important to keep in mind that regulatory requirements tend to change more often than statutory requirements. From a cybersecurity and data privacy perspective, regulatory compliance examples include:

- Defense Federal Acquisition Regulation Supplement (**DFARS**)
- Cybersecurity Maturity Model Certification (**CMMC**)
- Federal Acquisition Regulation (**FAR**)
- Federal Risk and Authorization Management Program (**FedRAMP**)
- DoD Information Assurance Risk Management Framework (**RMF**)
- National Industrial Security Program Operating Manual (**NISPOM**)
- Financial Industry Regulatory Authority (**FINRA**)
- New York Department of Financial Services (**NY DFS**) 23 NYCRR 500
- European Union General Data Protection Regulation (**EU GDPR**)

Contractual Obligations

Contractual obligations are required by legal contract between private parties. This may be as simple as a cybersecurity or data privacy addendum in a vendor contract that calls out unique requirements. It also includes broader requirements from an industry association that membership brings certain obligations. From a cybersecurity and privacy perspective, common contractual compliance requirements include:

- Payment Card Industry Data Security Standard (**PCI DSS**)
- ISO 27001 certification
- Service Organization Control (**SOC**) audits
- Generally Accepted Privacy Principles (**GAPP**)

[3] Unified Scoping Guide - https://content.complianceforge.com/unified-scoping-guide.pdf

- Center for Internet Security Critical Security Controls (**CIS CSC**)
- Cloud Security Alliance Cloud Controls Matrix (**CSA CCM**)

Defining What It Takes For Your Business Processes To Be Secure & Resilient

Cybersecurity and data protection controls that are not required by a law, regulation or contractual obligation are "nice to have" controls that are discretionary for an organization to implement. Any aspect of non-compliance with a discretionary control would be isolated within the realm of the stakeholder making the requirement, since the requirement is internal to your organization. The source of these discretionary requirements may be from:

- Board of Director (**BoD**) guidance;
- Steering Committee recommendations;
- Internal Audit findings;
- Third-party audit/assessment recommendations; and/or
- Internal staff preferences.

The importance of these discretionary controls is that those are often organization-specific considerations to mitigate risk that is specific to an organization's business practices.

Discretionary Cybersecurity & Data Protection Considerations

A common frustration amongst cybersecurity practitioners is about the gaps that exist in many "best practice" cybersecurity frameworks. This is often where there are complaints about organizations holding an ISO 27001 certification, SOC 2 audit or PCI DSS audit that still have breaches or security incidents, where the argument is that a certification does not mean the organization is secure. The remedy to such gaps is through discretionary cybersecurity & data protection controls that are not directly mandated by a compliance obligation, such as the requirements for:

- Data Loss Prevention (**DLP**)
- Network Access Control (**NAC**)
- File Integrity Monitoring (**FIM**)
- 24/7 Security Operations Center (**SOC**)
- Artificial Intelligence (**AI**) governance controls
- Sandboxing / detonation chambers
- Segmented Dev / Test / Production environments
- Cloud infrastructure-specific controls
- Embedded technology-specific controls

Discretionary Resilience Considerations

NIST defines resilience as, *"The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."*[4] From a discretionary control perspective, this may require the addition of technologies and processes to help ensure the continuity of business operations, such as:

- Continuity of Operations Plan (**COOP**)
- Business Continuity / Disaster Recovery (**BC/DR**) Plan
- Failover / redundancy capabilities
- Business continuity test exercises
- Offsite, online backup storage
- Offsite, offline backup storage
- Transactional-level backups

[4] NIST Glossary - https://csrc.nist.gov/glossary/term/resilience#

Defining Negligence As It Pertains To Cybersecurity & Data Privacy

The following content is leveraged from Cornell's Law School Legal Information Institute (**LII**)[5] 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 NIST SP 800-171 requirements under applicable DFARS clauses*);
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 entity being the source of the data breach*)

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

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

Determining A Breach Of Duty

When determining how whether the defendant has breached a duty, courts will usually use the *Learned Hand formula*[6], which is an algebraic approach to determining liability. If *B < PL*, then there will be negligence liability for the party with the burden of taking precautions where:

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

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

Determining Whether There Was A Duty To Act

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

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

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

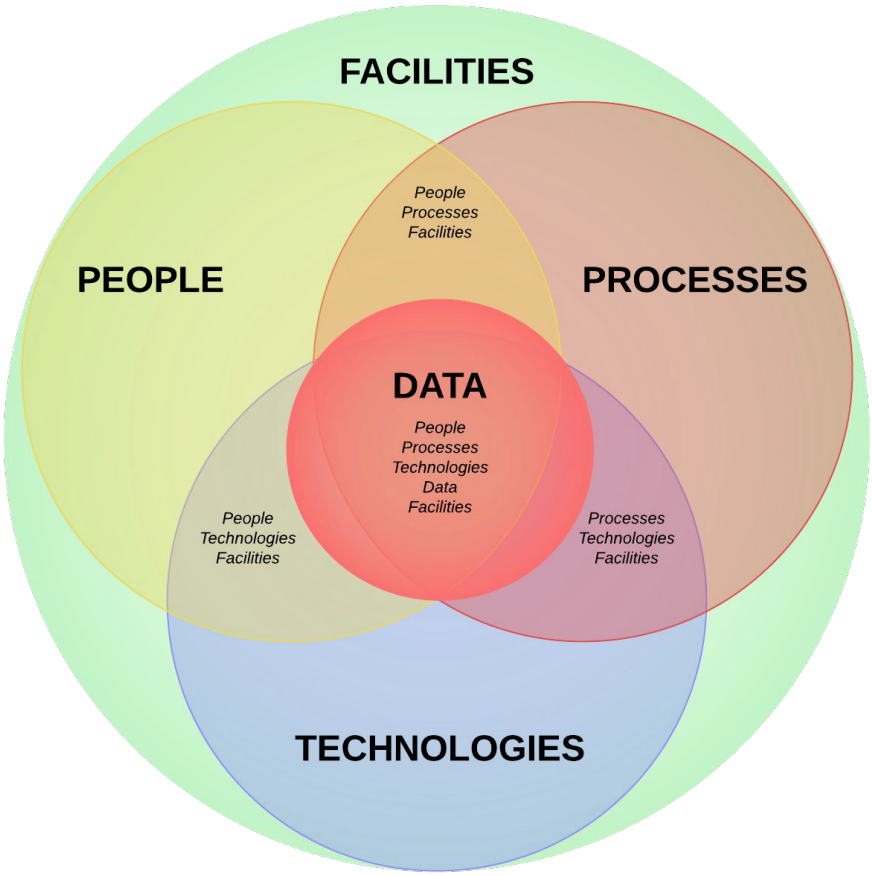
Holistic Approach To Address Control Applicability

Cybersecurity practitioners generally agree that the importance of robust cybersecurity and data protection controls cannot be overstated. However, the applicability of those controls is sometimes in question since not all controls are applicable. To help demonstrate the applicable nature of controls:

- An employee cannot have a secure baseline configuration applied.
- An Incident Response Plan (**IRP**) cannot sign a Non-Disclosure Agreement (**NDA**), use Multi-Factor Authentication (**MFA**) or be patched.
- You cannot apply end user training to a firewall.
- Sensitive / regulated data cannot be assigned roles and responsibilities.
- Your data center cannot undergo employee background screening.

People, Processes, Technology, Data & Facilities (PPTDF)

The People, Processes, Technology, Data and Facilities (**PPTDF**) model provides a comprehensive approach to address control applicability. These five (5) components provide a lens to view the applicability of controls.



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 aids in that process.

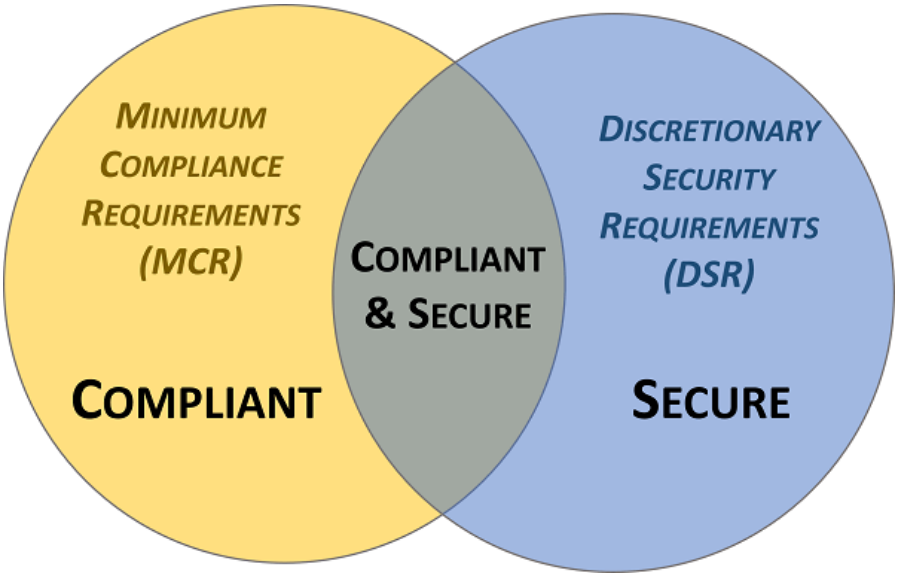
Similar in concept to Governance, Risk & Compliance (**GRC**) or Integrated Risk Management (**IRM**), ICM is focused on supporting processes and practices that must exist for a cybersecurity & data privacy program to operate effectively and efficiently. ICM is designed to proactively address the strategic,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

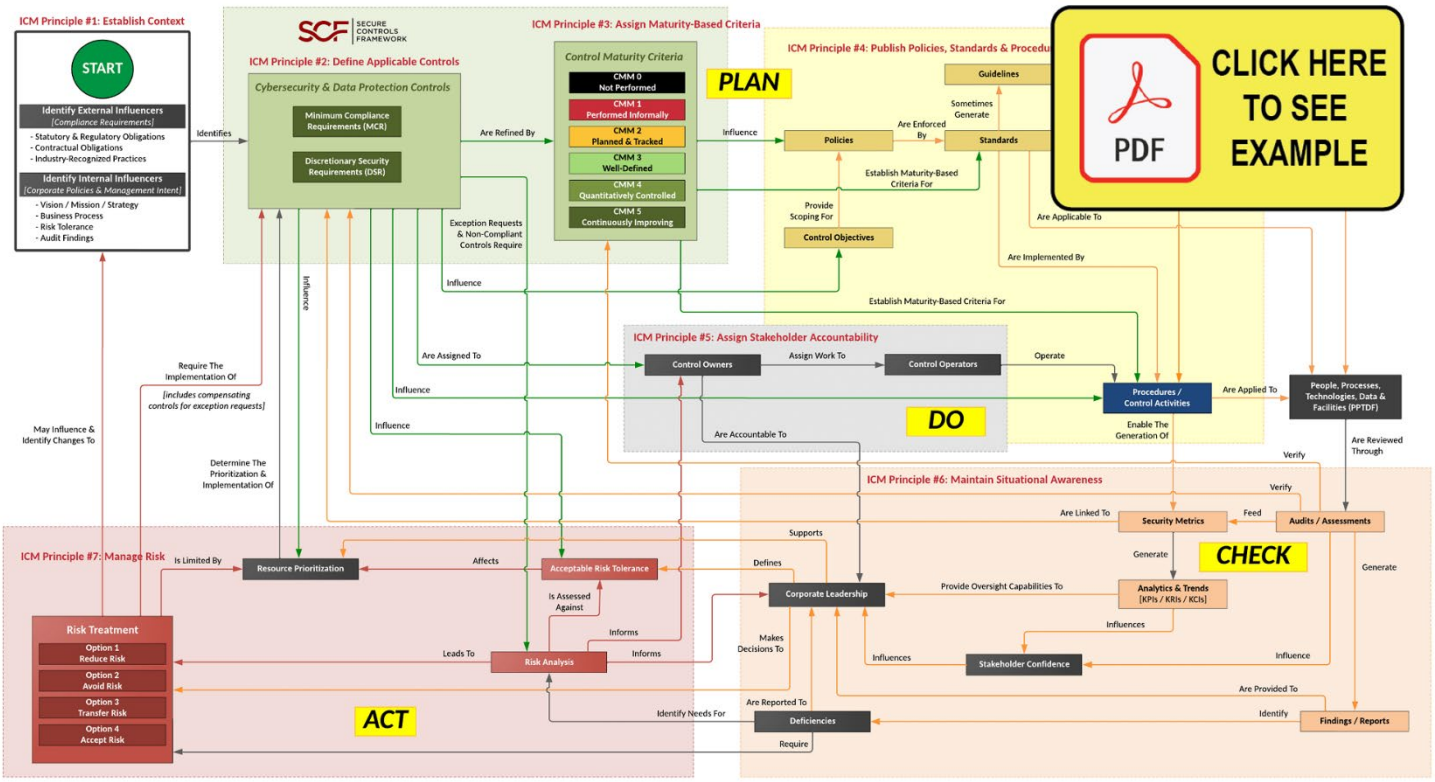
The combination of MCR and DSR equate to an organization's Minimum Security Requirements (**MSR**), which define the "must have" and "nice to have" requirements for People, Processes, Technology & Data (**PPTD**) in one control set. It defines the Minimum Viable Product (**MVP**) technical and business 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 both a due diligence and due care element of the cybersecurity & data privacy program, since context changes with time.

Things to consider when establishing context:

- Mission / vision / strategy of the organization;
- Statutory (law), regulatory (regulation) and contractual requirements for cybersecurity and data protection;
- Fiscal constraints;
- Organizational structure;
- Organizational risk appetite;
- Corporate culture (e.g., how receptive is the organization to change); and
- Geographic-specific requirements.

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.

Things to consider when defining applicable controls:

- Controls to address "must have" requirements from laws, regulations and contractual obligations to ensure the organization is compliant with its obligations;
- Controls to address "discretionary" requirements that exist to ensure the organization has secure and resilient operations; and
- There needs to be at least an annual review to ensure the applicable controls are accurate to the current needs for compliance, security and resilience.

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.

Things to consider when assigning maturity-based criteria:

- Not all controls need to be the same level of maturity, since each control has an associated cost. The higher level of maturity, the higher the cost. This is a risk management decision to define what right looks like for the organization;
- The expected level of maturity needs to at least comply with applicable statutory, regulatory and contractual requirements;
- Low-levels of maturity may be considered negligent behavior from a due care perspective.

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.

Things to consider when publishing policies & standards:

- The policies and standards need to reflect both the "must have" and "nice to have" requirements identified in Principle 2;
- Policies should be designed as "high level statements of management intent" and are not expected to change often; and
- Standards should be designed to assign granular requirements to enforce policies. As technologies change/evolve, those standards will need to change to ensure compliant, secure and resilient operations.

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.

Things to consider when assigning stakeholder accountability:

- Procedures are not "owned" by the cybersecurity or privacy teams. Procedures are the responsibility of the control owner / operator; and
- The NIST NICE Cybersecurity Workforce Framework is a methodology to identify cybersecurity and data privacy-related roles and associated responsibilities.[7]

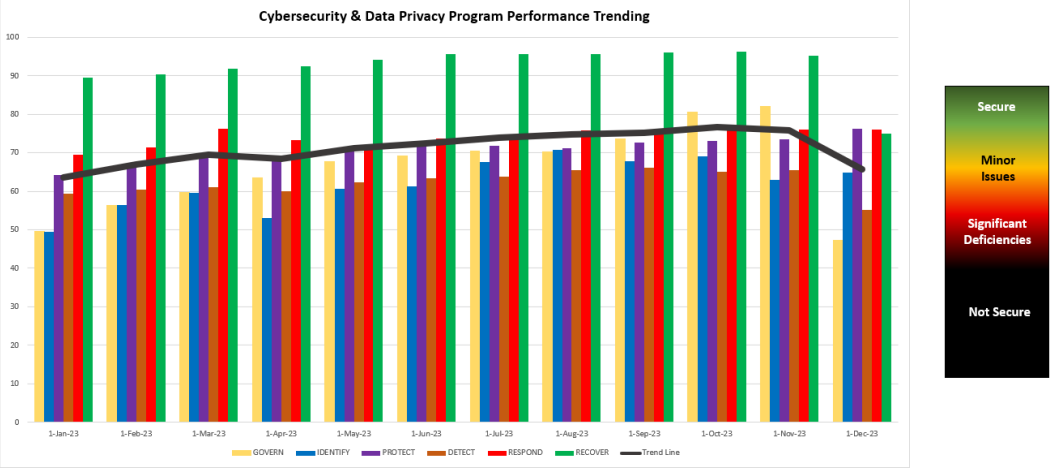
[7] NIST NICE - https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

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.

Things to consider when maintaining situation awareness:

- Metrics/analytics are meant to tell the long-term story of how the cybersecurity and data privacy program is doing. The historical performance provides context to an organization's senior leaders; and
- The metrics/analytics needs to be tied to measurable controls that can help eliminate Fear, Uncertainty and Doubt (**FUD**) reporting.



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.

Things to consider when managing risk:

- Traditional risk management practices have four (4) options to address identified risk:
  - Reduce the risk to an acceptable level;
  - Avoid the risk;
  - Transfer the risk to another party; or
  - Accept the risk.
- To provide the context of which option is viable for an organization, there needs to be defined risk tolerance.

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.

Things to consider when evolving processes:

- Changes in the compliance landscape (e.g., laws, regulations and contractual obligations);
- Technology changes; and
- Budget/resourcing constraints that affect how processes are implemented.

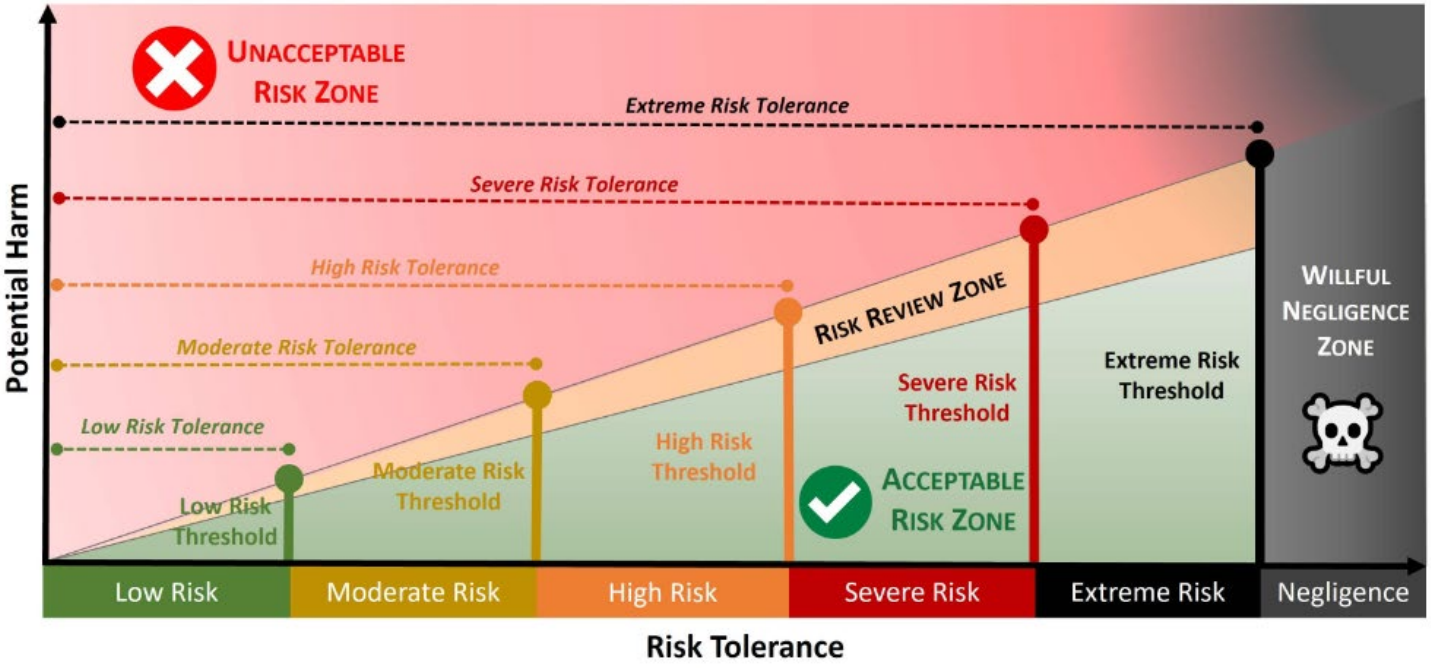
PRACTICAL RISK MANAGEMENT CONSIDERATIONS

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.

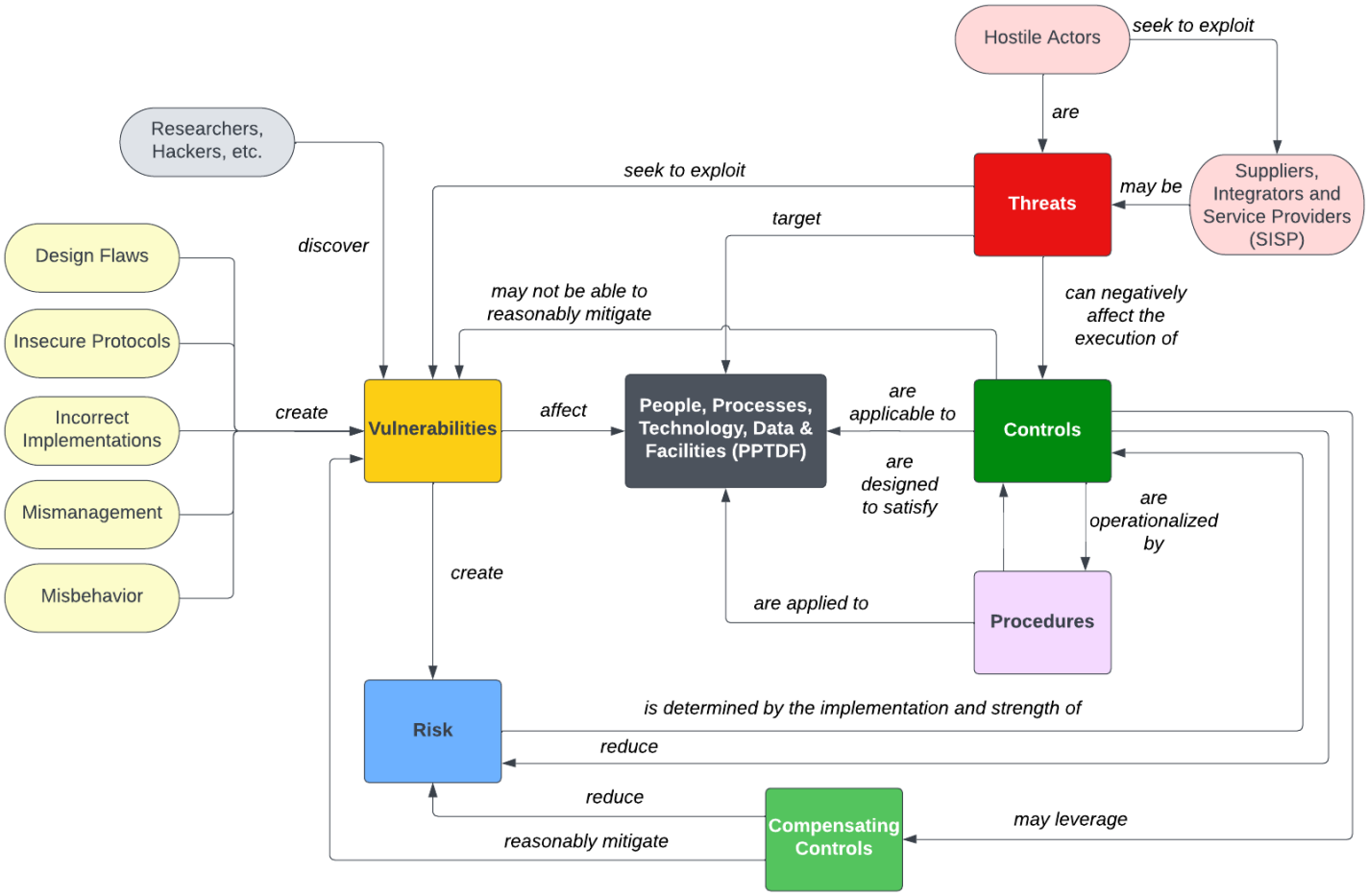
RISK MANAGEMENT OPTIONS

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:[8]



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.*

[8] *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:[9]

- 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. [10]

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).

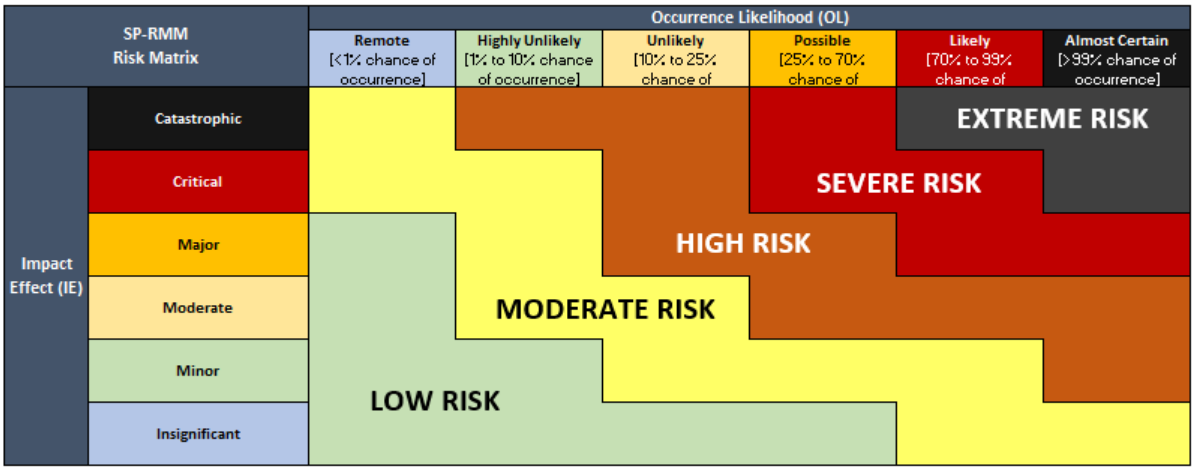
From a graduated scale perspective, it is possible to define "tolerable" risk criteria to create five (5) useful categories of risk:

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**).

[9] *PMBOK® Guide - https://www.pmi.org/pmbok-guide-standards/foundational/pmbok*
[10] *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.

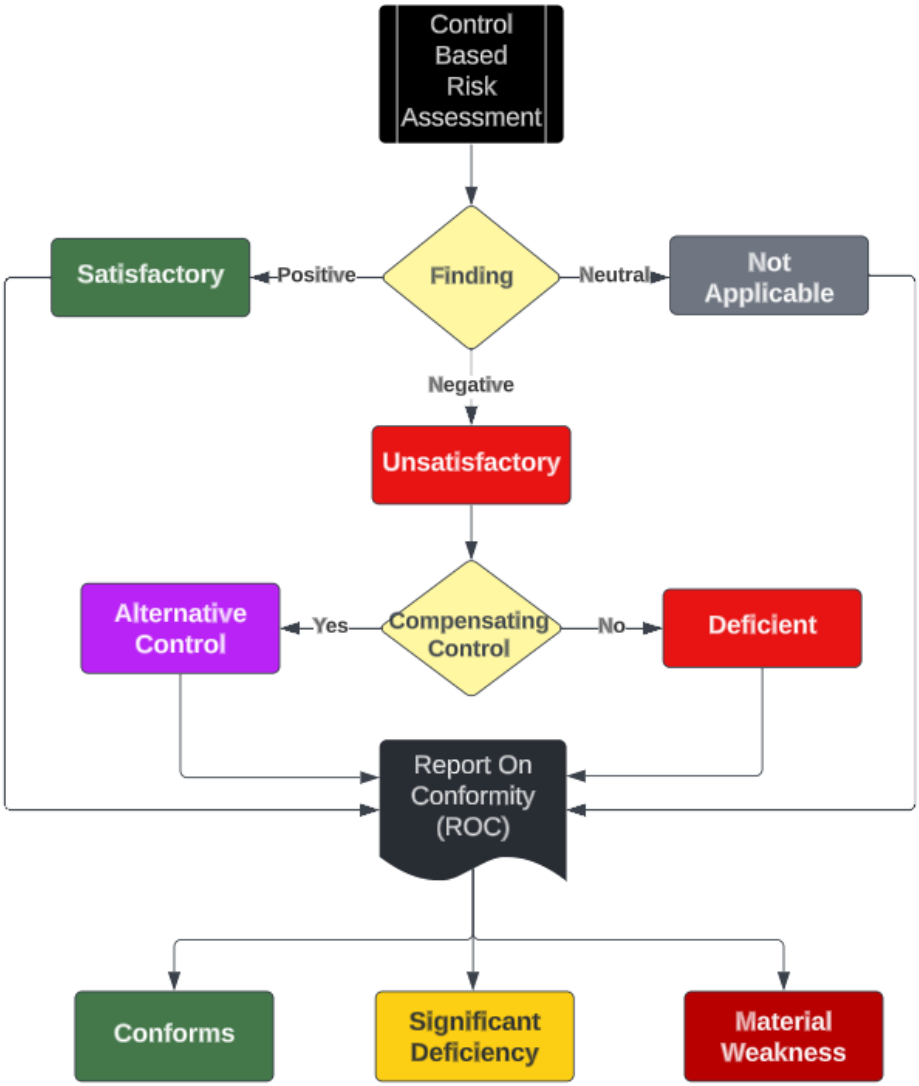
When an organization goes through some form of "certification" process, it undergoes a conformity assessment (e.g., ISO 27001, CMMC, SOC 2, PCI DSS, RMF, etc.). Conformity assessments are designed to assure that a particular product, service, or system meets a given level of quality or safety. Instead 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."*[11]

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."*[12]
- 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."*[13]

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

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

- 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.

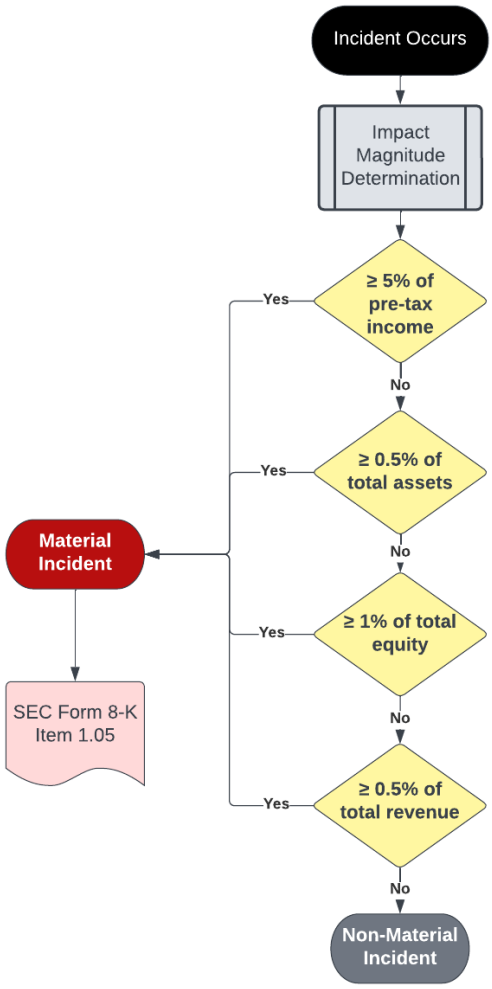
Materiality Thresholds

The SEC, Generally Accepted Accounting Principles (**GAAP**) and International Financial Reporting Standards (**IFRS**) lack specificity in defining the criteria for materiality. Therefore, organizations generally have leeway to define it on their own. The lack of authoritative definition for materiality is not unique, since the concept of risk appetite, risk tolerance and risk threshold also suffer from nebulous definitions by statutory and regulatory authorities.

For an item to be considered material, the control deficiency, risk, threat or incident (singular or a combination) generally must meet one or more of the following criteria where the potential financial impact is:[14]

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

This materiality determination can be visualized with this infographic with the callout for publicly traded companies having a requirement to publicly disclose material cybersecurity incidents: [15]



Applying ICM To Governance, Risk Management & Compliance (GRC) Functions

[14] *Norwegian Research Council - https://snf.no/media/yemnkmbh/a51_00.pdf*
[15] *SEC Cybersecurity Final Rule - https://www.sec.gov/files/rules/final/2023/33-11216.pdf*

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.[16] 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

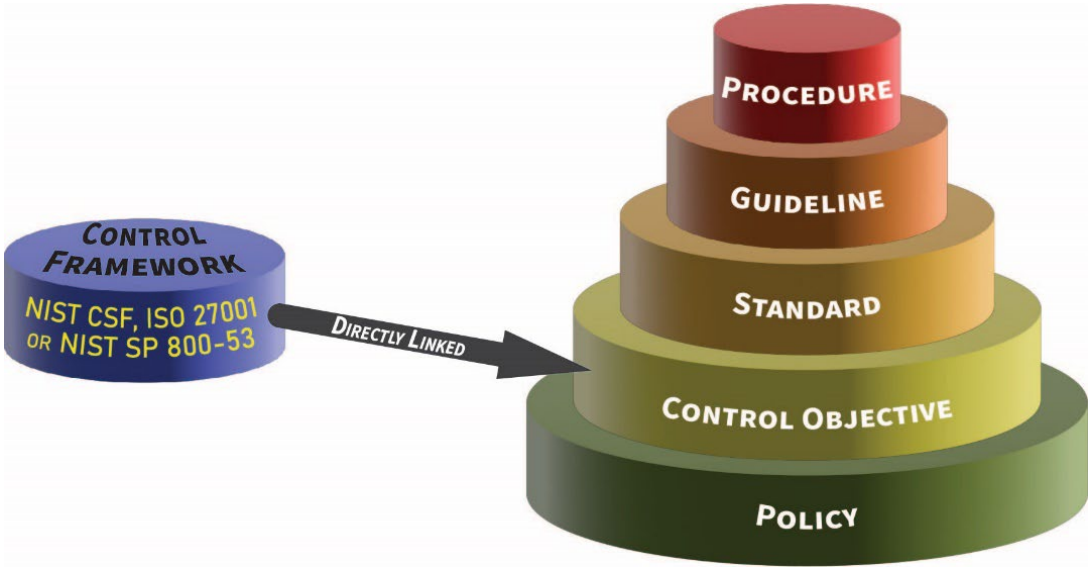
[16] OCEG – What is GRC - https://www.oceg.org/ideas/what-is-grc/

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.

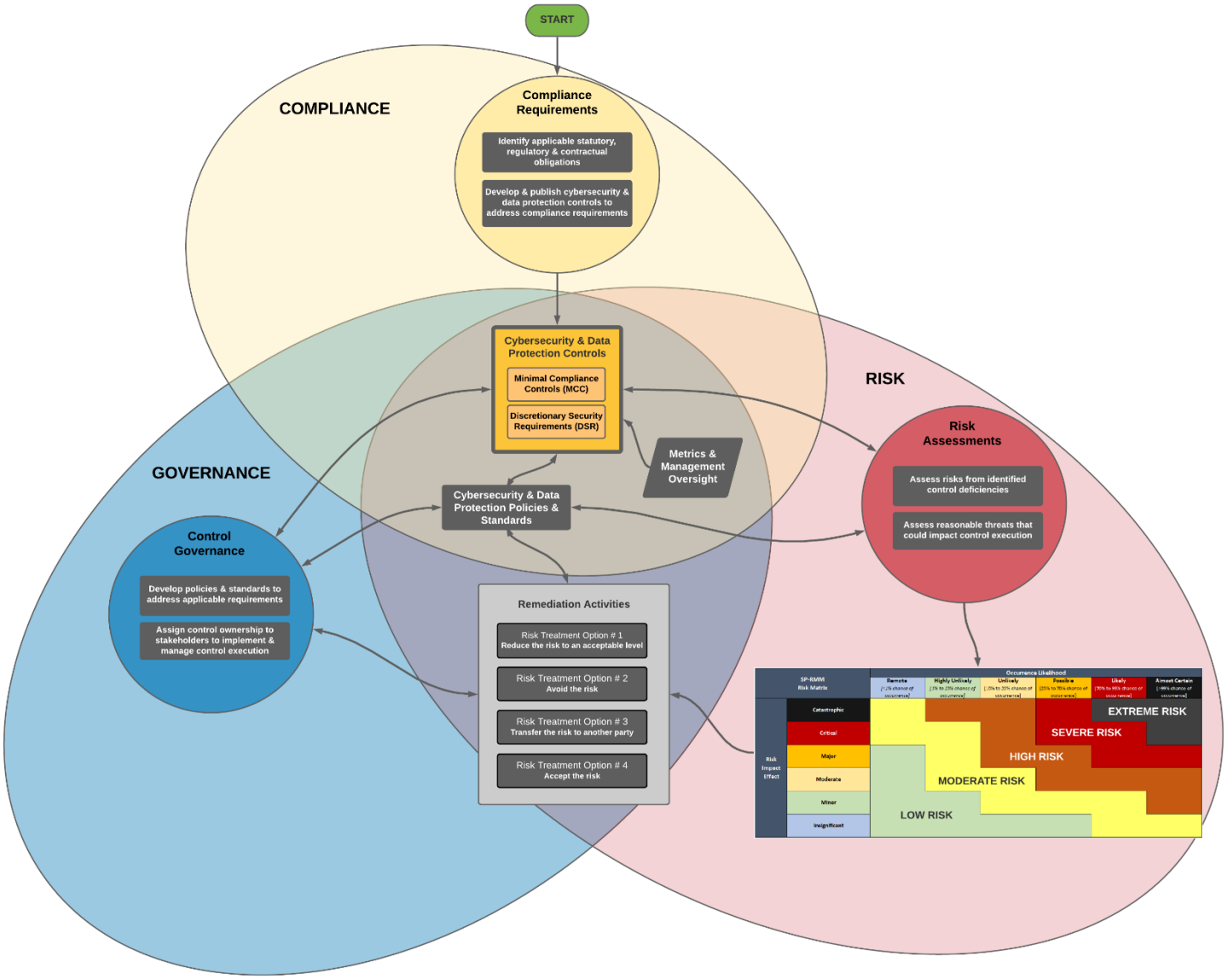
While Risk Management personnel do not perform the actual remediation actions (that is the responsibility of the control owner), Risk Management assists in determining the appropriate risk treatment options:

- 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.

CYBERSECURITY & DATA PROTECTION CONTROLS

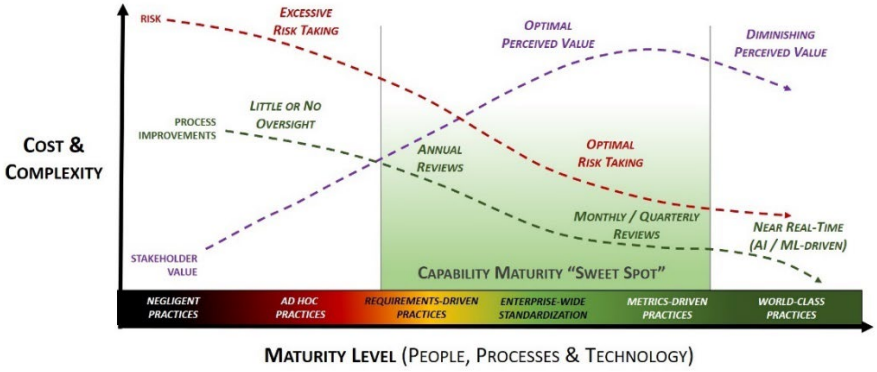
While it is possible to use any control set, ICM was specifically designed based on the comprehensive nature of the Secure Controls Framework (**SCF**). The SCF has thirty-two (32) domains that address cybersecurity & data privacy-related requirements. The SCF is licensed according to Creative Commons,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

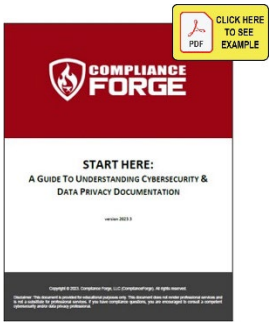
- The C|P-CMM is based on the Systems Security Engineering Capability Maturity Model (**SSE-CMM**); and
- Each SCF control has entries for CMM level 0 through level 5 pre-populated to provide maturity-based guidance on controls.



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.[17]

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.

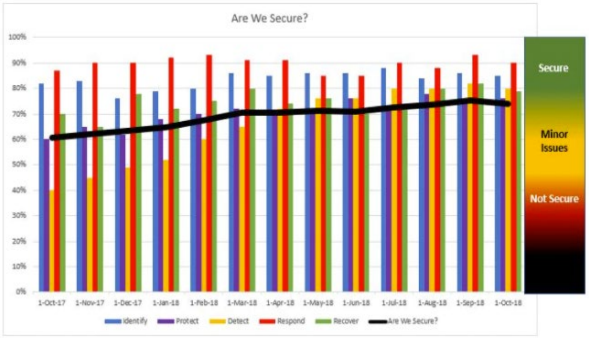
The best starting point is the NIST SP 800-181, *Workforce Framework for Cybersecurity (NICE Framework)*.[18] The NICE Framework offers an efficient way to assign stakeholder accountability for internal and external stakeholders.

[17] ComplianceForge – A Guide To Understanding Cybersecurity & Data Privacy Documentation - https://content.complianceforge.com/Understanding-Cybersecurity-Data-Protection-Documentation.pdf
[18] NIST SP 800-181 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

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 Cybersecurity Metrics Reporting Model™ (**CMRM**) 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 (**KPX**) as a way to logically-organize and report individual metrics. Using KPX enables the SMRM to provide a reasonable and defendable answer.

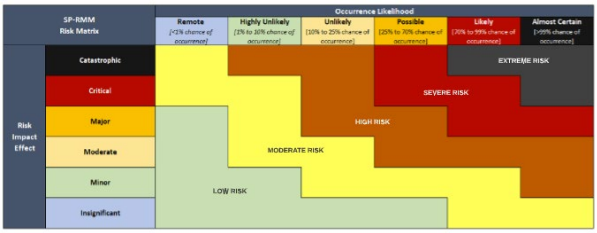


Manage Risk

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.

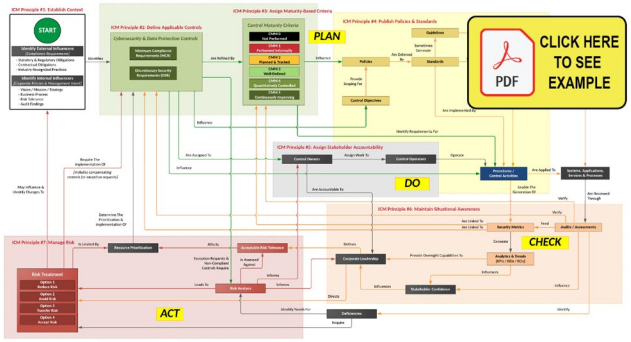
The value of the C|P-RMM is having a standardized methodology where controls are tied to specific risks and threats. Based on the other criteria offered by the SCF (e.g., weighting and maturity criteria), the C|P-RMM makes calculating risk a straightforward process.



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]