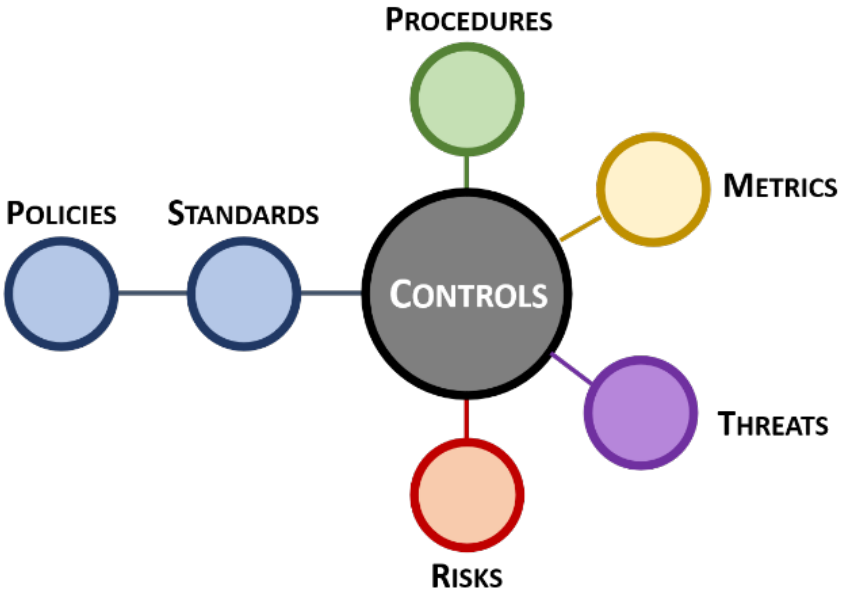
Integrated Controls Management (ICM) Model

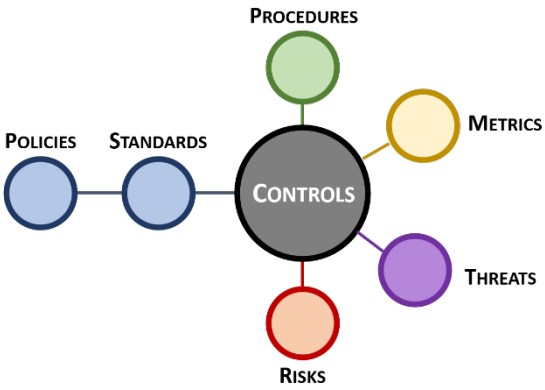


Version 2024.5

Table of Contents

EXECUTIVE SUMMARY – A "HOW TO GRC PLAYBOOK"

The ICM is designed to be a "how to GRC" playbook to establish or refine Governance, Risk Management and Compliance (GRC) practices.

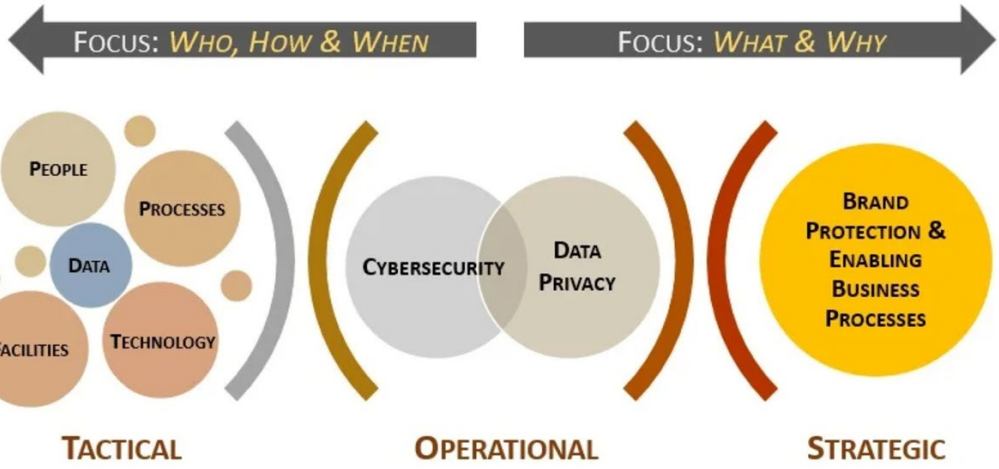


The premise of ICM model is that controls are central to cybersecurity & data privacy operations, as well as the overall business rhythm of an organization. This premise of the ICM is supported by the **Cybersecurity & Data Privacy Risk Management Model (C|P-RMM),**[1] that describes the central nature of controls, where not just policies and standards map to controls, but procedures, metrics, threats and risks, as well.

The ICM model is controls-centric, where controls are viewed as the nexus, or central pivoting point, for an organization's cybersecurity & data privacy operations.

> ***"ICM is 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 Cybersecurity Supply Chain Risk Management (C-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 **(e.g., mandatory requirements)**. 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 **(e.g., discretionary requirements)**. 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/*

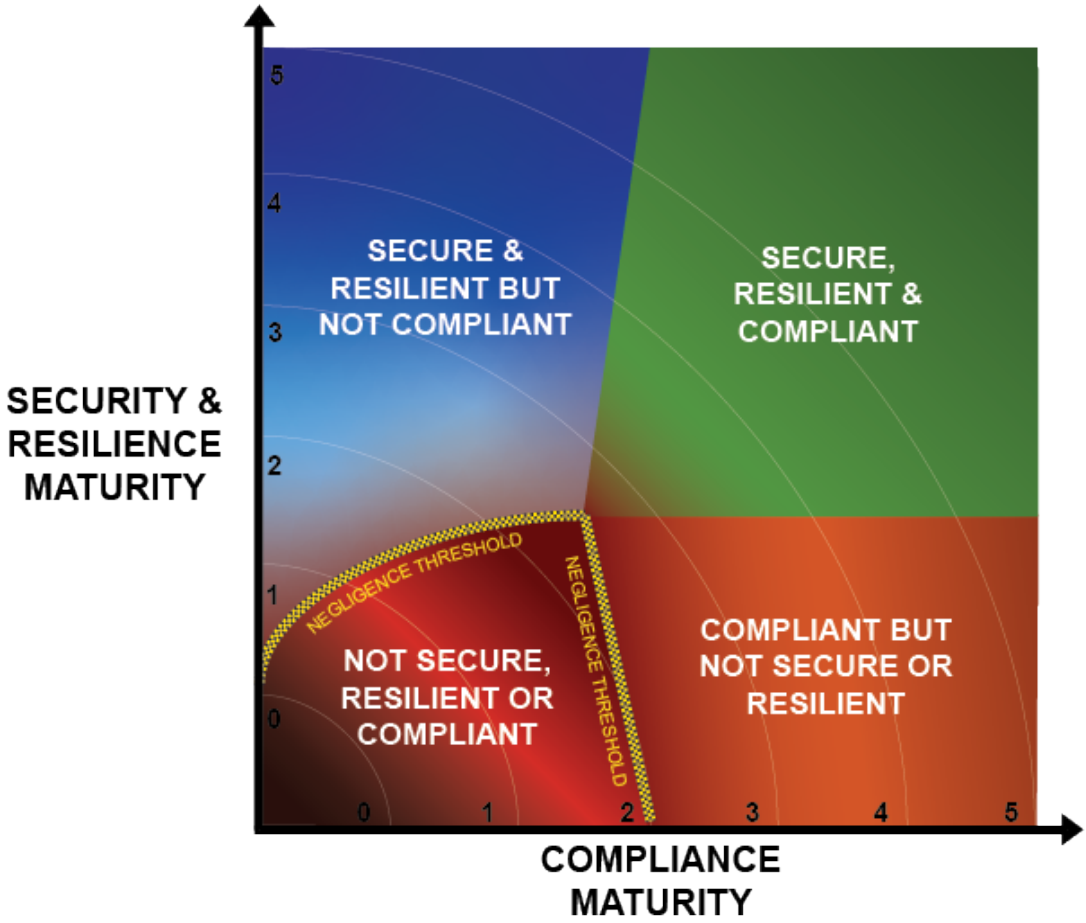
SECURITY VS COMPLIANCE

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 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/*

Holistic Approach To Address Control Applicability

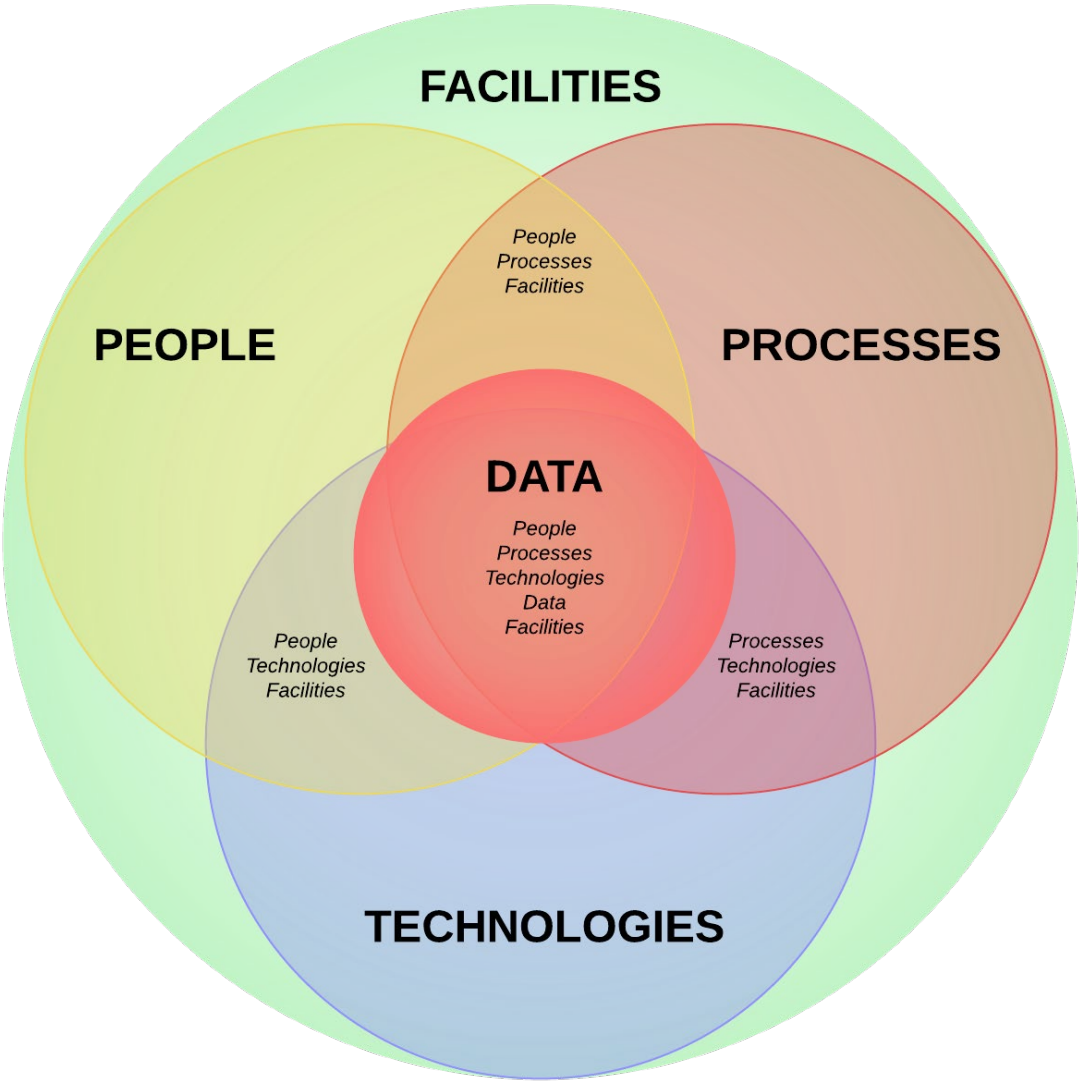
Cybersecurity practitioners generally agree that the importance of robust cybersecurity and data protection controls cannot be overstated. However, the applicability of those controls is sometimes in question since not all controls are applicable. To help demonstrate the applicable nature of controls:

- 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:

1. **People**. Control directly applies to humans (e.g., training, background checks, non-disclosure agreements, etc.).
2. **Processes**. Control directly applies to administrative work performed (e.g., processes, procedures, administrative documentation, etc.).
3. **Technologies**. Control directly applies to systems, applications and services (e.g., secure baseline configurations, patching, etc.).
4. **Data**. Control directly applies to data protection (e.g., encrypting sensitive and/or regulated data, applying metatags, etc.).
5. **Facilities**. Control directly applies to infrastructure assets (e.g., physical access, HVAC systems, visitor control, etc.).



DEFINING NEGLIGENCE AS IT PERTAINS TO CYBERSECURITY & DATA PROTECTION PRACTICES

The following content is leveraged from Cornell's Law School Legal Information Institute (LII)[3] 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., requirement to comply with NIST SP 800-171 to protect Controlled Unclassified Information (CUI) as part of a contract*);
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*[4], 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.

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

INTEGRATED CONTROLS MANAGEMENT (ICM) MODEL

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."*

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.

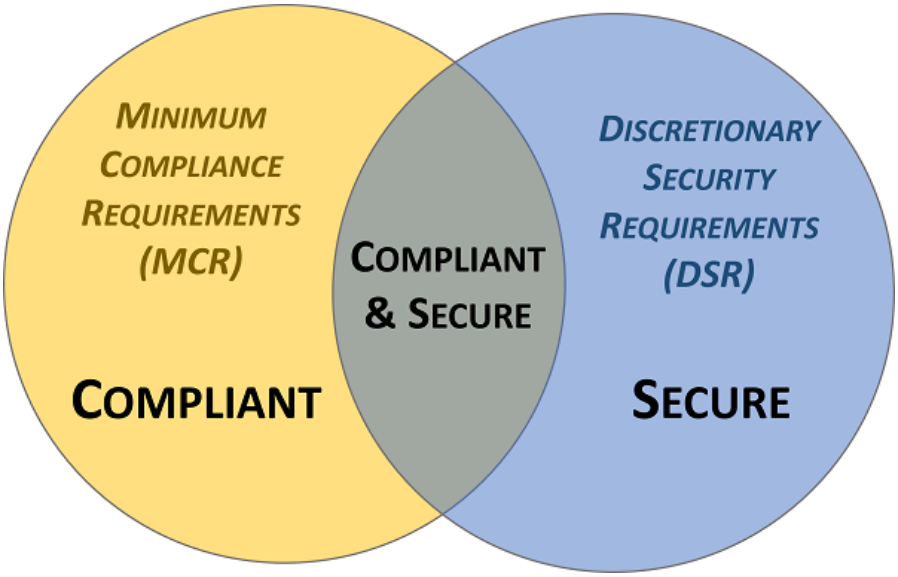
In practical terms, controls exist to protect an organization's data. Requirements for asset management do not primarily exist to protect the inherent value of the asset, but the data it contains, since assets are merely data containers. Assets, such as laptops, servers and network infrastructure are 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.

DEFINING WHAT IT MEANS TO BE BOTH 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:

- **Minimum Compliance Requirements (MCR)** are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts **(e.g., mandatory requirements)**. 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 **(e.g., discretionary requirements)**. 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.



ESTABLISHING 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 PPTDF 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.

MUST HAVE CONTROLS - *DEFINING "BEING COMPLIANT"* THAT IS SPECIFIC TO YOUR BUSINESS PROCESSES

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.[5]

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:

- Process owners;
- Procurement / Contracts Management;
- Project Management Office (PMO);
- 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 include 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)

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

- 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
- Contractual requirement to adhere to a specific set of requirements, such as:
  - NIST Cybersecurity Framework
  - Generally Accepted Privacy Principles (GAPP)
  - Center for Internet Security Critical Security Controls (CIS CSC)
  - Cloud Security Alliance Cloud Controls Matrix (CSA CCM)

NICE TO HAVE CONTROLS - *DEFINING* "SECURE & RELIANT" THAT IS SPECIFIC TO YOUR BUSINESS PROCESSES

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."*[6] 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)

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

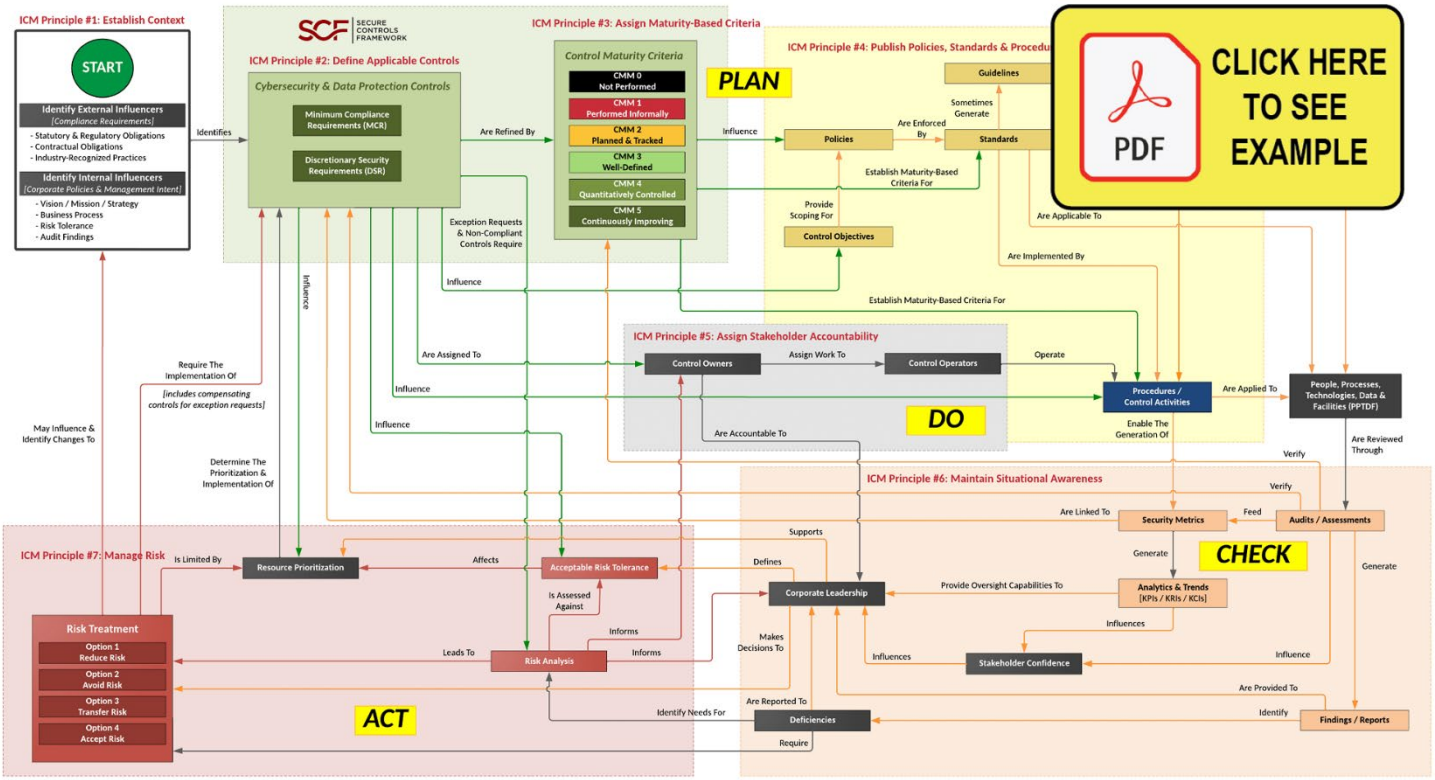
- Business Continuity / Disaster Recovery (BC/DR) Plan
- Failover / redundancy capabilities
- Business continuity test exercises
- Offsite, online backup storage
- Offsite, offline backup storage
- Transactional-level backups

ICM Principles – Plan, Do, Check & Act (PDCA) Approach To GRC Operations

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 (ICM model)



[graphic download - https://securecontrolsframework.com/content/Plan-Do-Check-Act.pdf]

ICM 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.

ICM Principle 1 Implementation Guidance

Part of your due diligence process is to establish the context of the scope for cybersecurity & data privacy controls. Practical steps to establish context includes:

- Read through the C|P principles to familiarize yourself with the thirty-three (33) domains to understand how they come together to address the cybersecurity, privacy and physical security considerations for a modern security program.
- Talk with representatives outside of IT and cybersecurity to gain an appreciation of other compliance requirements (e.g., legal, procurement, physical security, etc.).
- Come up with a list of the "must have" laws, regulations and frameworks that your organization must comply with.
- Come up with a list of "nice to have" requirements that your Board of Directors, or other stakeholders, feel are necessary.

Understanding the requirements for both cybersecurity & data privacy principles involve a simple process of distilling expectations. This process is all part of documenting reasonable expectations that are "right-sized" for an organization, since every organization has unique requirements.

Some people freak out and think they must do all 1,200+ controls in the SCF and that is just not the case. It is best to visualize the SCF as a "buffet of cybersecurity & data privacy controls," where there is a selection of 1,200+ controls available to you. Just as you do not eat everything possible on a buffet table, the same applies to the SCF's control set. Once you know what is applicable to you, you can generate a customized control set that gives you just the controls you need to address your statutory, regulatory and contractual obligations.

The approach looks at the following spheres of influence to identify applicable SCF controls:

- Statutory obligations - These are laws (e.g., US state, federal and international laws).
- Regulatory obligations - These are requirements from regulatory bodies or governmental agencies.
- Contractual obligations - These are requirements that are stipulated in contracts, vendor agreements, etc.
- Industry-recognized practices - These are requirements that are based on an organization's specific industry that are considered reasonably-expected practices.

Please keep in mind that the SCF is a tool and is only as good as its used – just like a pocketknife shouldn't be used as a prybar. Realistically, if you do not scope the controls from the SCF correctly, you will not address your applicable compliance requirements since you are missing what is expected. That is not a deficiency of the SCF – that is simply negligence on the part of the user of the tool.

To make sure scoping is done properly, it is imperative for you to speak with your legal, IT, project management, cybersecurity and procurement teams (and other stakeholders you may feel are relevant to scoping controls). The reason for this collaboration is so that you can get a complete picture of all the applicable laws, regulations and frameworks that your organization is legally obligated to comply with. Those teams will likely provide the best insights into what is required, and this list of requirements will then make it simple to go through and customize the SCF for your specific needs!

ICM 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:

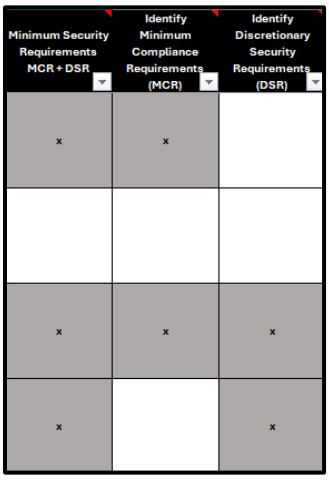
- Controls to address "must have" requirements from laws, regulations and contractual obligations to ensure the organization is compliant with its obligations;
- Controls to address "discretionary" requirements that exist to ensure the organization has secure and resilient operations; and
- There needs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

ICM Principle 2 Implementation Guidance

NOTE: This guidance is specific to the Secure Controls Framework (SCF) for control refinement. The SCF is fundamentally an Excel spreadsheet. Therefore, you can use your Excel skills to manually filter the requirements. If you are comfortable with Excel, it might take you 5-10 minutes to do this filtering, based on how many requirements you need to map to. Within the SCF, there is a column labelled "Minimum Security Requirements (MSR) MCR + MSR" that will assist you in this process.

Follow these steps to tailor the SCF:

1. Either hide or delete all of the columns containing laws, regulations or frameworks that are not applicable to your organization (e.g., if you only have to comply with ISO 27002, PCI DSS and EU GDPR, then you can delete or hide all other mapping columns but those).Using the filter option in Excel (little gray arrow on the top row in each column), you would then filter the columns to only show cells that contain content (e.g., don't show blank cells in that column).
2. A selection of either MCR or DSR will automatically select the MSR + DSR column:
    a. In the MCR column, simply put an "x" to mark that control as being "must have" controls.
    b. In the DSR column, simply put an "x" to mark that control as being "nice to have" controls.
3. Unfilter the column you just performed this task on and do it to the next law, regulation or framework that you need to map.
4. Repeat steps 2 and step 3 until all your applicable laws, regulations and frameworks are mapped to.



The MSR + DSR column will now have an "x" that marks each SCF control that is applicable for your needs, based on what was selected for MCR and DSR controls. This will leave you with a SCF control set that is tailored for your specific needs.

ICM 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, Technologies, Data & Facilities (PPTDF) 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 the 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; and
- Lower levels of maturity may be considered negligent behavior from a due care perspective.

ICM Principle 3 Implementation Guidance

From the previous step, you identified the controls that are applicable to your specific needs (e.g., MCR + DSR). You can now use the SP- CMM criteria to "define what right looks like" for each control. This is further explained in the Cybersecurity & Data Privacy Capability Maturity Model (C|P-CMM).[7]

The C|P-CMM draws upon the high-level structure of the Systems Security Engineering Capability Maturity Model v2.0 (SSE-CMM), since we felt it was the best model to demonstrate varying levels of maturity for PPTDF at a control level. If you are unfamiliar with the SSE-CMM, it is well-worth your time to read through the SSE-CMM Model Description Document that is hosted by the US Defense Technical Information Center (DTIC).

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

ICM 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.

ICM Principle 4 Implementation Guidance

There are generally three (3) options to obtain 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.

NOTE: ComplianceForge is a SCF Licensed Content Provider (LCP) and has editable policies, standards and procedures templates that are based on the SCF.

ICM 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.[8]

ICM Principle 5 Implementation Guidance

Assigning stakeholder accountability offers unique challenges for organizations, since it is beyond IT, cybersecurity & data privacy. Common stakeholders involve Human Resources (HR), procurement, facilities management, legal and many other teams to ensure accountability is enforceable. Realistically, this step is an executive-management function since it requires inter-departmental enforcement by organizational management.

A great starting point is the NIST SP 800-181, *Workforce Framework for Cybersecurity (NICE Framework)*.[9] The NICE Framework offers an efficient way to assign stakeholder accountability for internal and external stakeholders.

[8] *NIST NICE - https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center*
[9] *NIST SP 800-181 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf*

ICM Principle 6: Maintain Situational Awareness

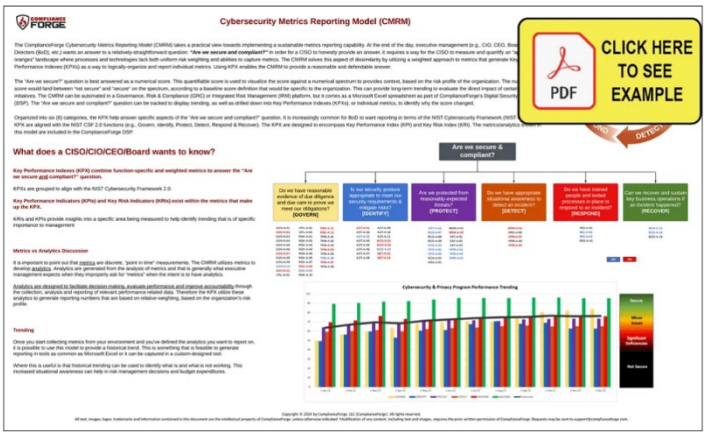
Situational awareness must involve more than merely "monitoring controls" (e.g., metrics). While metrics are a point-in-time snapshot into discrete controls' performance, the broader view of metrics leads to a longer-term trend analysis. When properly tied in with current risk, threat and vulnerability 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.

ICM Principle 6: Implementation Guidance

Maintaining situational awareness has different meanings, based on the security culture of an organization. Metrics / analytics reporting is plagued by the Garbage In, Garbage Out (GIGO) problem. Often the GIGO issue is rooted in executives trying to explain their perceived needs for metrics to cybersecurity practitioners in a way that describes the design of a "football bat" (e.g., nonsensical solution).



ComplianceForge's Cybersecurity Metrics Reporting Model (CMRM) takes a practical view towards implementing a sustainable metrics reporting capability. [10] At the end of the day, executive management often just wants a simple answer to a relatively-straightforward question: "Are we secure?"

ICM 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.

ICM Principle 7 Implementation Guidance

There are many ways to manage risk. However, the SCF's Cybersecurity & Data Privacy Risk Management Model (C|P-RMM) contains a control-centric:[11]

- Risk catalog;
- Threat catalog; and
- Methodology to not only perform a risk assessment, but manage risk across the organization.

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.

---

[10] *Cybersecurity Metrics Reporting Model (CMRM) - https://complianceforge.com/content/pdf/complianceforge-cybersecurity-metrics-reporting-model.pdf*

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

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 of risk management terminology.

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 into 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, this leaves remediation, transferring or avoiding as the remaining three (3) options, since accepting the risk would be prohibited.

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.

ICM 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.

ICM Principle 8 Implementation Guidance

Without an overarching concept of operations for the broader GRC/IRM function, organizations will often find that their governance, risk management, compliance and privacy teams are siloed in how they think and operate. These siloed functions and unclear roles often stem from a lack of a strategic understanding of how these specific functions come together to build a symbiotic working relationship between the individual teams that enables quality control over PPTDF.

The ICM model 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 in which 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.

APPLYING THE ICM MODEL TO EXISTING 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, while help provide the ability to safely navigate 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 safely. 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

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 PPTDF 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.[12] 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, Concept of Operations (CONOPS) documents, etc.; and
- By the Risk Management team to assess risk.

Given that 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.

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

GOVERNANCE

Based on these controls, Governance has two (2) key functions:

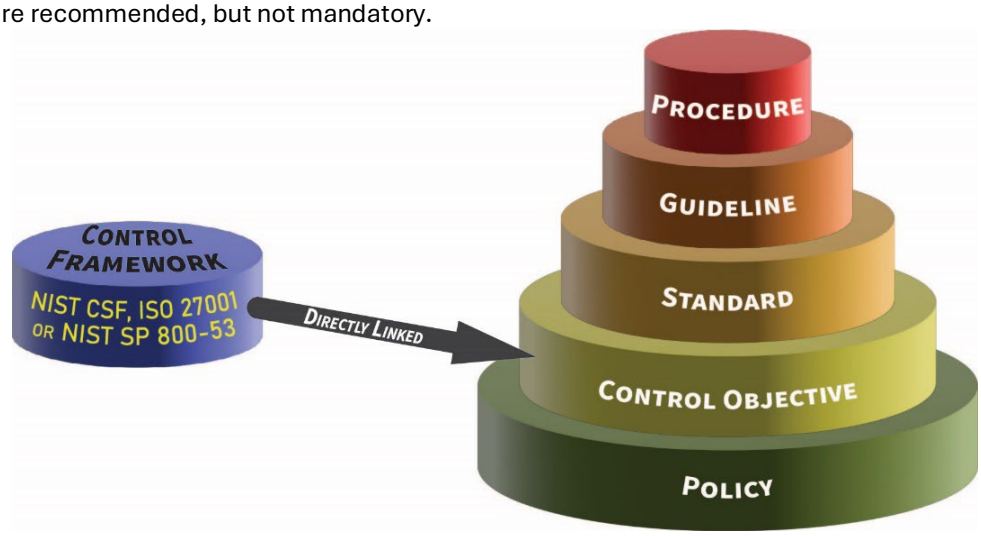
- Develop policies and standards to meet those compliance obligations (defined by applicable control objectives); and
- Assign ownership of those controls to the applicable stakeholders involved in the affected business processes. This process often requires a documented Responsibility, Accountability, 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 organization's 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.

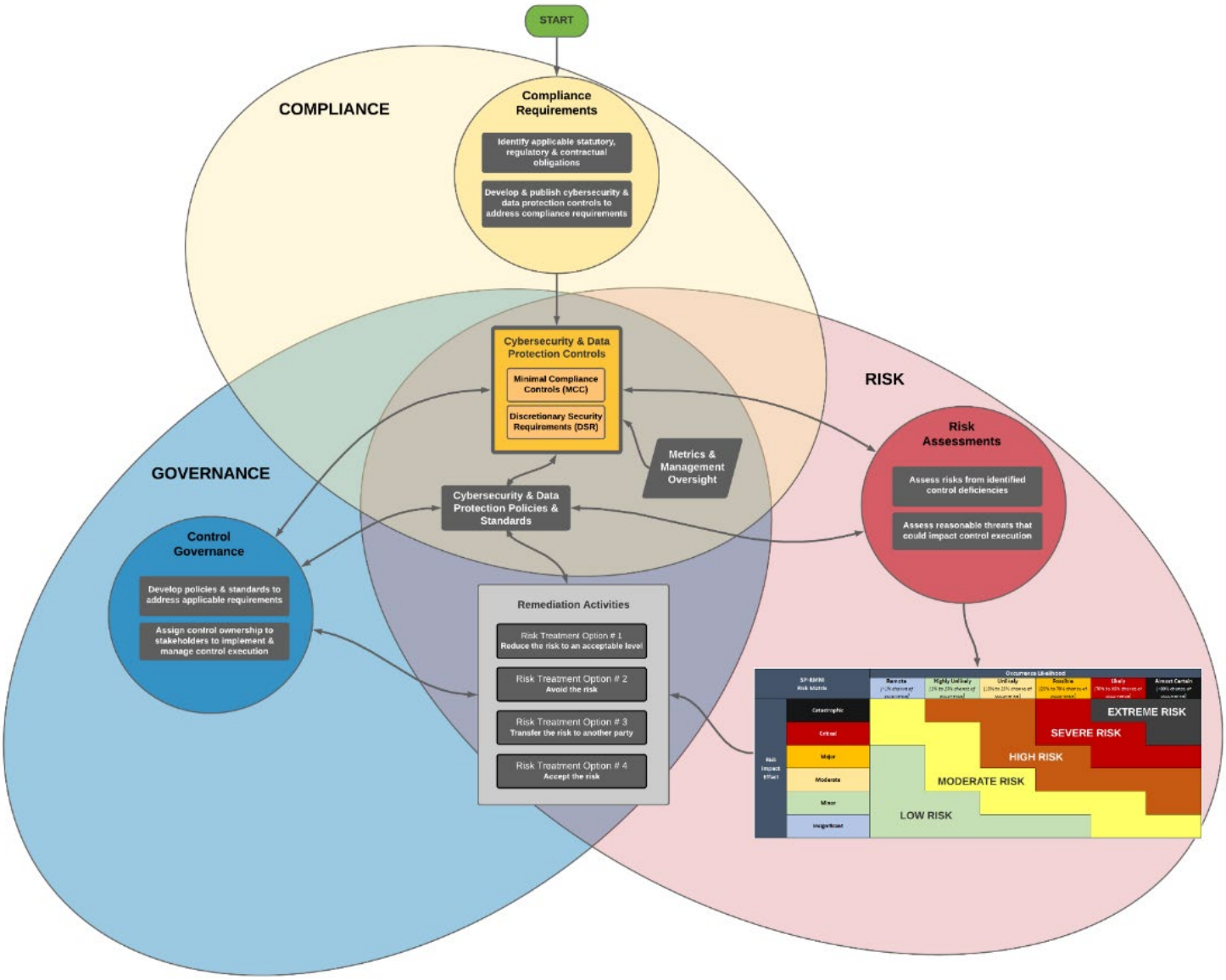
While Risk Management personnel do not perform the actual remediation actions (that is the responsibility of the control owner), Risk Management assists in determining the appropriate risk treatment options:

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



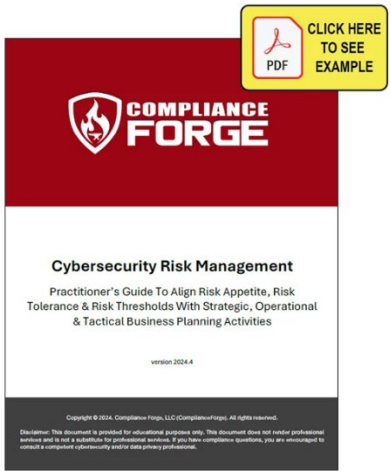
[graphic download - https://securecontrolsframework.com/content/GRC-Fundamentals.pdf]

PRACTICAL CYBERSECURITY RISK MANAGEMENT CONSIDERATIONS

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

PRACTITIONER'S GUIDE TO CYBERSECURITY RISK MANAGEMENT

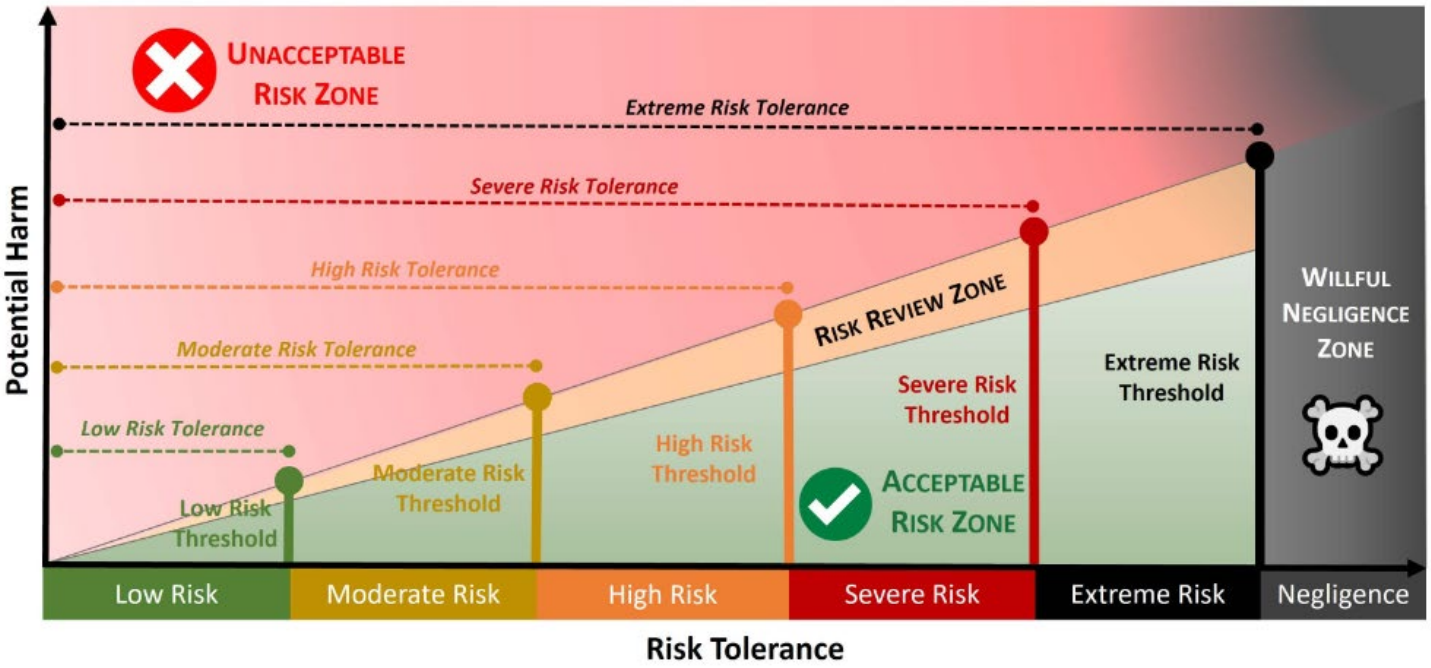
A useful guide to gain an insightful understanding of cybersecurity risk management practices is the **Cybersecurity Risk Management: Practitioner's Guide To Align Risk Appetite, Risk Tolerance & Risk Thresholds With Strategic, Operational & Tactical Business Planning Activities.**[13]



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.



[13] *Cybersecurity Risk Management* - https://complianceforge.com/content/pdf/cybersecurity-practitioners-guide-to-risk-management.pdf