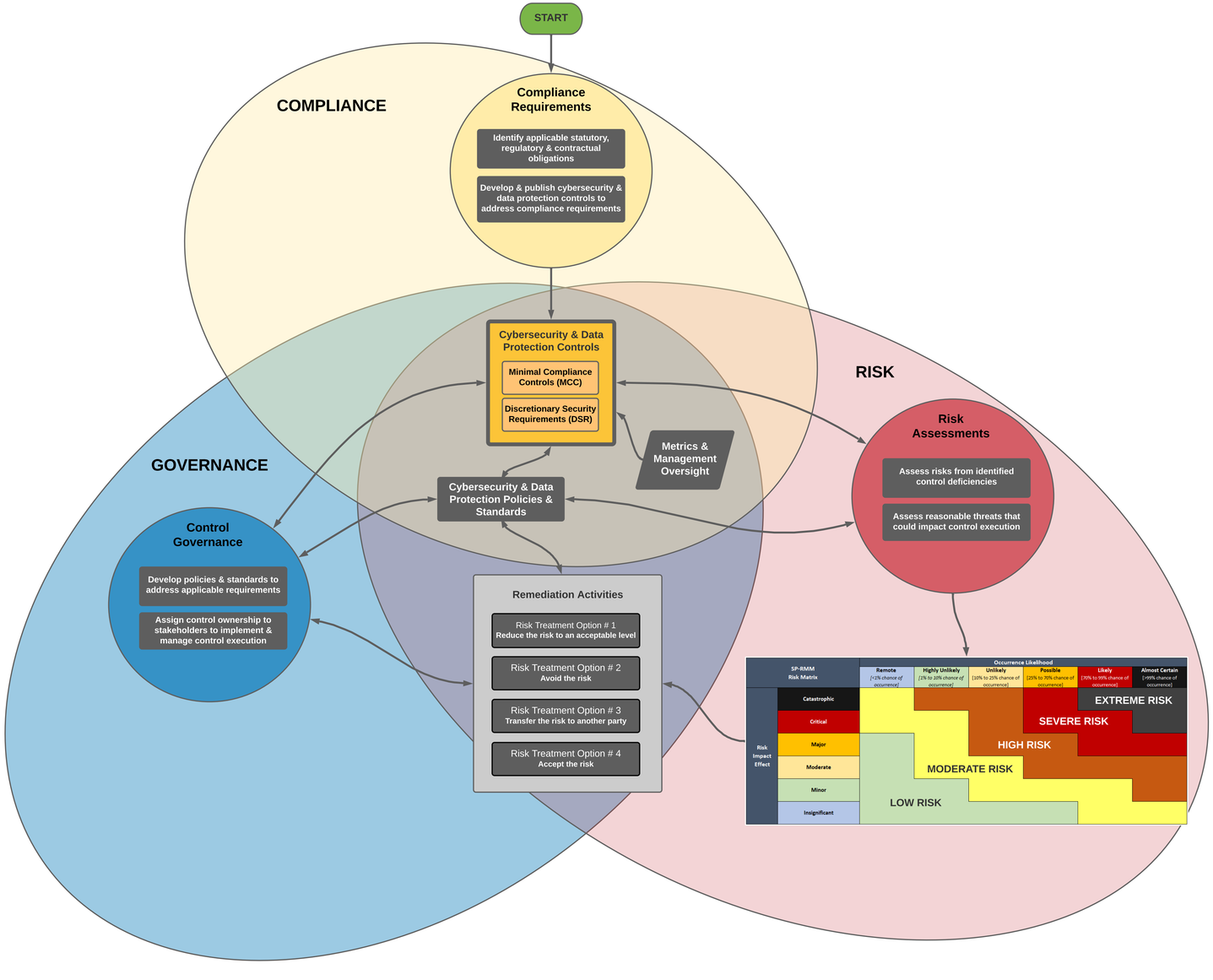
Integrated Controls Management (ICM): *Controls-Centric Governance, Risk Management & Compliance (GRC)*

2022.1



GRC Interactions Explained

The processes described below can be visualized in the diagram shown below that shows the interrelated nature of Governance, Risk Management and Compliance (**GRC**) functions to build and maintain an organization's cybersecurity and privacy program. When you seek to establish an Integrated Controls Management (**ICM**) approach to security, it can be viewed in the traditional view of GRC functions. However, it is important to note that these fundamental GRC function components must be implemented in order of precedence to get the process properly focused.

At the heart of GRC processes are controls. Controls are the "security glue" that make processes, applications, systems and services compliant and/or secure. It is important to note that controls are not static, since business processes are not static. As business processes evolve, so must the applicable cybersecurity and data protection controls to ensure secure and compliant practices are properly identified and maintained. This process of defining "what right looks like" for controls is divined from determining the following:

- Minimum Compliance Criteria (**MCC**) are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCC's are primarily externally-influenced, based on statutory, regulatory and contractual requirements. These are the "must have" controls for an organization to be considered compliant. MCC should never imply adequacy for secure practices and data protection, since MCC are merely compliance-related.
- Discretionary Security Requirements (**DSR**) are tied to the organization's risk appetite since DSR are "above and beyond" MCC, where the organization self-identifies additional cybersecurity and data protection 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 MCC establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

1. 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 and data protection 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 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, 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 exceeds what a single framework can address, so the organization has to leverage some form of metaframework (e.g., framework of frameworks).

Compliance defines the controls necessary to meet the organization's specific needs (e.g., MCC + DSR) and publishes one or more control sets (e.g., specific to a project/contract/law/regulation or organization-wide controls). This 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 and data protection 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.

2. 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 and data protection 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 and data protection 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.

3. 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 to maintain situational awareness so the organization to remains 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 and data protection controls (e.g., MCC + 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. This is why 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 and requiring management to own their risk management decisions, it can help the organization maintain its target risk threshold.

COMPLIANCE FORGE
www.ComplianceForge.com

SCF SECURE CONTROLS FRAMEWORK
www.SecureControlsFramework.com