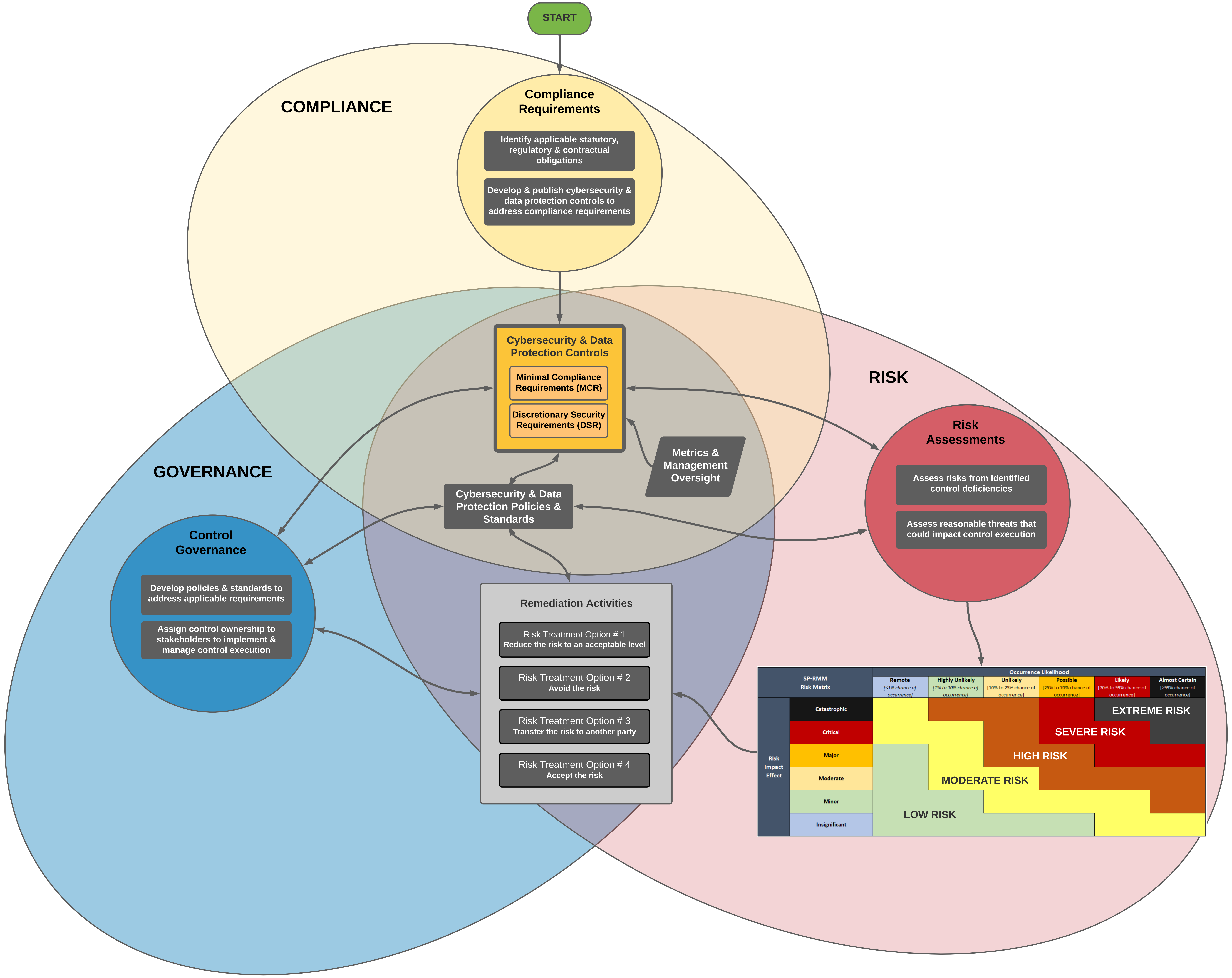
Governance, Risk & Compliance (GRC) Fundamentals

2025.1


START
COMPLIANCE
Compliance Requirements
Identify applicable statutory, regulatory & contractual obligations
Develop & publish cybersecurity & data protection controls to address compliance requirements
Cybersecurity & Data Protection Controls
Minimal Compliance Requirements (MCR)
Discretionary Security Requirements (DSR)
Metrics & Management Oversight
RISK
Risk Assessments
Assess risks from identified control deficiencies
Assess reasonable threats that could impact control execution
GOVERNANCE
Control Governance
Develop policies & standards to address applicable requirements
Assign control ownership to stakeholders to implement & manage control execution
Cybersecurity & Data Protection Policies & Standards
Remediation Activities
Risk Treatment Option # 1
Reduce the risk to an acceptable level
Risk Treatment Option # 2
Avoid the risk
Risk Treatment Option # 3
Transfer the risk to another party
Risk Treatment Option # 4
Accept the risk

SP-RMM Risk Matrix		Occurrence Likelihood					
		Remote [<1% chance of occurrence]	Highly Unlikely [1% to 10% chance of occurrence]	Unlikely [10% to 25% chance of occurrence]	Possible [25% to 70% chance of occurrence]	Likely [70% to 99% chance of occurrence]	Almost Certain [>99% chance of occurrence]
Risk Impact Effect	Catastrophic	🟨	🟧	🟧	🟥	⬛ EXTREME RISK	⬛
	Critical	🟨	🟨	🟧	🟥 SEVERE RISK	🟥	⬛
	Major	🟩	🟨	🟧 HIGH RISK	🟧	🟥	🟥
	Moderate	🟩	🟨 MODERATE RISK	🟨	🟧	🟧	🟧
	Minor	🟩	🟩	🟨	🟨	🟨	🟧
	Insignificant	🟩 LOW RISK	🟩	🟩	🟩	🟨	🟨

GRC Function Integrations

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 a GRC program, 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:

1. COMPLIANCE. GRC practices start with the need to first identify applicable statutory, regulatory and contractual obligations that the organization must comply with, as well as internal business requirements (e.g., Board of Director directives). This is a COMPLIANCE function and not a "risk assessment," where it is more of a fact-finding exercise to define requirements. This process of identifying statutory, regulatory and contractual obligations addresses due diligence expectations for an organization to identify what is reasonably required to address its applicable external compliance obligations from a cybersecurity and data protection perspective.

It is important to note that controls sets 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:

- **Minimum Compliance Requirements (MCR)** are the absolute minimum requirements that must be addressed to comply with applicable laws, regulations and contracts. MCR's are primarily externally-influenced, based on industry, government, state and local regulations. MCR should never imply adequacy for secure practices and data protection, 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 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 MCR establish the foundational floor that must be adhered to, DSR are where organizations often achieve improved efficiency, automation and enhanced security.

The premise of Integrated Controls Management (ICM) is that controls are central to the cybersecurity and privacy operations, as well as the business rhythms of the organization. Without properly defining MCR and DSR thresholds, an organization's overall cybersecurity and 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.

2. GOVERNANCE. Once the controls are defined to meet the organization's specific needs (e.g., MCR + DSR), an effective GOVERNANCE implementation must:
1. Develop policies and standards to meet those compliance obligations; and
2. 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.

The development and implementation of the policies and standards is evidence of due diligence that the organization's compliance obligations are built into administrative, technical and physical security requirements. It is important to ensure that policies and standards document what the company is doing, as the policies and standards are often the mechanisms by which outside regulators measure implementation and maturity of the control. 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. 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.

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 SOP, and the ensuing deliverables that are produced as a part of executing procedures, generate evidence of due care that reasonable practices are in place and operating accordingly.

3. RISK MANAGEMENT. While RISK MANAGEMENT comes after COMPLIANCE and GOVERNANCE functions in establishing an ICM program, RISK MANAGEMENT is integral in maintaining situational awareness for the organization to remain both secure and compliant. RISK MANAGEMENT activities addresses both due diligence and due care obligations to identify, assess and remediate control deficiencies. RISK MANAGEMENT functions must align with GOVERNANCE practices for exception management (e.g., compensating controls). Additionally, COMPLIANCE must evaluate findings from internal audits, risk assessments and third-party assessments to determine if adjustments to the organization's cybersecurity and data protection controls (e.g., MCR + DSR) are necessary, based on business process changes, technology advancements and/or an evolution of the organization's risk threshold. RISK MANAGEMENT is crucial to be able to maintain situational awareness for cybersecurity and privacy operations.

In the end, once a GRC program is implemented, it requires regular and on-going reassessment of GOVERNANCE, RISK MANAGEMENT and COMPLIANCE activities to maintain both an appropriate balance between these processes and effective operations. Similar to a three-legged stool, if one leg is too short or too long, the program will be unbalanced, wobble and not operate as needed. GRC requires strong and active support of organizational leadership to ensure secure and compliant practices are implemented and maintained.

COMPLIANCE FORGE
www.ComplianceForge.com

SCF SECURE CONTROLS FRAMEWORK
www.SecureControlsFramework.com