# Governance Risk and Compliance

Cybermcbean

PODCAST

G|RC

**Gordon Mc Bean Certified Ethical Hacker (CEH)**

**Web:** www.cybermcbean.com
**Youtube Channel:** www.youtube.com/@gmmcdigital1976

**November 6Th, 2025**


# Governance, Risk and Compliance

## Introduction:

In this evolving cyber world Governance, Risk, and Compliance (GRC) guidelines is crucial for effectively managing cybersecurity risks and ensuring compliance with regulations.

As cyber threats evolve, organizations must adopt a proactive approach to GRC and continually adjust to advancements and digital transformations.

GRC safeguards against various cyber threats by offering a structured approach to managing governance, compliance, and cybersecurity risk.

By adopting and implementing GRC in cybersecurity, organizations can enhance their security posture and performance and achieve their business goals and outcomes.

**Governance, Risk, and Compliance (GRC)** is a framework organizations use to align IT with business goals, manage risks effectively, and ensure compliance with regulations.

Governance, Risk and Compliance. It refers to an organization's strategy for handling the interdependencies and alignment between three essential components of modern digital organizations:

- Organization Governance policies
- Organization Risk management programs
- Organization Compliance

Not long ago, most organizations practiced Governance, Risk and compliance separately, today organizations realize that when Governance, Risk and Compliance are combined in a single coordinated model. This unified approach helps reduce wastage, increase efficiency, reduce noncompliance risk and share information more effectively.

## Governance Overview:


**Governance**, is the responsibility of senior management and the board of directors and focuses on creating the mechanism an organization uses to ensure that personnel follow established processes and policies.

**Governance** is an organization's set of policies, rules designed to achieve its goals. It defines the responsibilities of key stakeholders, the board of directors and senior management. Good governance covers principles such as ethics, accountability, transparency, conflict resolution policies and resource management.

## The importance of governance:

1. Addressing the increase for civil or legal liability as a result of information inaccuracy.
2. Providing assurance of policy compliance.
3. Increasing predictability and reducing uncertainty of business operations.
4. Providing the structure and framework to optimize allocations of limited security resources

5. Ensuring a level of assurance that critical decisions are not based on faulty information.
6. Ensuring a firm foundation for efficient and effective risk management, process improvement, rapid incident response and business continuity management.
7. Building greater confidence with trading partners
8. Improving trust in customer relationships.
9. Protecting the organization's reputation.
10. Providing accountability for safeguarding information during critical business activities, such as mergers, acquisitions, recovery and regulatory response.
11. Effective management of information security resources.

In order to achieve significant improvement in information security, the board of directors and senior management must be held accountable for information security governance.

### Governance objective:

**The objective of information security governance** is to develop, implement and manage security program that achieves the following outcome:

1. **Strategic alignment** – Aligning information security with business strategy in order to support organizational objectives.
2. **Risk Management** – Put in place appropriate measures to mitigate risk and reduce potential impacts on resources to an acceptable level.
3. **Value Delivery** – optimizing security investments in support of business objectives.
4. **Resource Optimization** – Using information security knowledge and infrastructure efficiently and effectively.
5. **Performance Management** – Monitoring and reporting on security processes to ensure objectives are achieved.

**Effective Governance:**

Information security governance is the responsibility of the board of directors and senior management.

Security governance is required to address legal and regulatory requirements.

## Risk Management:

**Risk Management** is the process by which an organization manages risk to acceptable levels within acceptable tolerances, identifies potential risk and its associated impacts, and prioritizes their mitigation based on the organization's business objective.

Risk exists wherever and whenever there's an opportunity for compromise, threat or loss.

ISO 31000 defines risk as "the effect of uncertainty on objectives." Risk affords opportunities for benefit (upside) or perils to success (downside).
Risk and opportunity go together. To provide value to stakeholders, enterprises must engage in activities and initiatives (opportunities), all of which carry degrees of uncertainty and, therefore, risk.
Managing risk and opportunity is a critical strategic activity for enterprise success.

## Risk = Probability x Severity

**Probability** is the likelihood of an event occurring, and severity is the extent and cost of the resulting loss.

**Risk management** identifies, assesses and controls threats to an organization's capital and earnings.

**Risk management** creates outcomes that inform decisions for addressing risks and minimizing the adverse effects of risk on an organization.

**The consequences of threats** can be either objective or quantifiable, like lost revenue and data theft, or subjective and difficult to quantify, such as damage to reputation and lost customer trust.

**Risk** must be considered in the decision-making process and committing the required resources to control and mitigate the identified risk, organizations can protect themselves from uncertainty, prioritize investments, reduce costs and increase business continuity.

**NOTE:**

**Objective** refers to information based on verifiable facts and evidence, rather than personal opinions or feelings. **Quantifiable** means that something can be expressed as an amount, quantity, or numerical value, making it measurable.

**Strategies to manage Identified Risk:**

1. Avoid the threat.
2. Reducing the negative effect or probability of the threat.
3. Transferring or sharing all or part of the threat with another party.
4. Retaining some or all of the potential or actual consequences of a particular risk if the anticipated gain is greater than the cost.

**Risk Management Strategies enable organization to:**

1. Consider potential risks or events before they occur
2. Establish procedures to avoid threats.
3. Understand and control risk so organization leadership is more confident in their decision-making process.
4. Create a safe and secure environment for employees and customers.
5. Increase the stability of operations while decreasing legal liability.
6. Protect the organization from events that are detrimental to the organization.
7. Establish insurance needed to save the organization on unnecessary premiums.

**Risk Assessment:**

Risk assessment is the process of identifying, analyzing and evaluating threats and vulnerabilities.

When establishing an information security program, conducting a risk assessment is key to identifying the needs of the organization and developing a security strategy.

In the cybersecurity, risk assessments are essential for identifying how external threat actors or insiders, could compromise sensitive information.

**Risk assessment** is performed to identify and quantify threats to information assets that are selected by the first step, valuation.

**1.** Identify assets and create a baseline
This phase identifies critical assets and prioritizes them to define the risk based on the criticality and value of each system. This creates a good baseline for vulnerability management.

**2.** Vulnerability scan
This phase is very crucial in vulnerability management. In this step, the security analyst performs the vulnerability scan on the network to identify the known vulnerabilities in the organization's infrastructure.

**3.** Risk assessment
In this phase, all profound uncertainties associated with the system are assessed and prioritized, and remediation is planned to eliminate system flaws permanently. The risk assessment summarizes the vulnerability and risk level identified for each of the selected assets.

**4.** Remediation
Remediation is the process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. This phase is initiated after the successful implementation of the baseline and assessment steps.

**5.** Verification
In this phase, the security team performs a re-scan of systems to assess if the required remediation is complete and whether the individual fixes have been applied to the impacted assets.

**6.** Monitor
Organizations need to perform regular monitoring to maintain system security. They use tools such as IDS/IPS and firewalls. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved.

## Compliance:

**Compliance** is the process that records and monitors the policies, procedures and controls needed to ensure that policies and standards are adequately adhered to.

Compliance means that a company adheres to the applicable rules and laws. This includes both country specific laws and requirements.

**Compliance Monitoring and Enforcement:**

**Policy Compliance:**

1. Policies must be comprehensive enough to cover all situations in which information is handled, yet flexible enough to allow for different processes and procedures to evolve for different technologies and still be in compliance.
2. It is necessary to designate formal security roles that establish which department head is responsible for putting processes in place that maintain security policy compliant and meet the appropriate standards for a given set of information systems.
3. **It is the responsibility of the Information Security Manager** to ensure that, in the assignment process, there are no orphan systems or systems without policy compliance owners.
4. **It is the responsibility of the Information Security Manager** to provide oversight and ensure that policy compliance processes are properly designed.

Strong understanding of relevant regulations and compliance frameworks (e.g., NIST, FIPS, ISO/IEC, PCI DSS).

## Organization Detection and monitoring capabilities on how to monitor and detection capabilities

### IDS – Intrusion Detection System:

An **Intrusion Detection System (IDS)** is a security tool that monitors network traffic and system activity for suspicious or malicious behavior. It detects and alerts administrators when it identifies potential threats, but it does not typically block them

### An Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) monitors network traffic in real-time, comparing it against known attack patterns and signatures, and blocking malicious activity or traffic that violates network policies. In short, an IPS is a security technology that proactively prevents unauthorized access, malicious activities, and potential threats within a network

**Security information and event management (SIEM)** technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other events and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).

**NOTE:**

Contextual data sources provide additional information that helps to understand the circumstances, environment, or background of a primary data point. They enrich the primary data, giving it more meaning and relevance.

**Governance risk and Compliance framework and methodologies:**


**COBIT 5** provides a comprehensive framework for the governance and management of enterprise IT and extensively addresses IT security, governance, risk and information security in general.

**COBIT 5 is based on five key principles:**

Principle 1: Meeting Stakeholder needs
Principle 2: Covering the Enterprise End-to-end
Principle 3: Applying a Single, Integrated Framework
Principle 4: Enabling a Holistic Approach
Principle 5: Separating Governance from Management

**COBIT 5 Process Assessment Model (PAM)**

The **COBIT 5** Process Assessment Model (PAM) is a tool that can be used to assess the current state and define a future desired state for Information Security.

**Capability Maturity Model Integration – also used in the Gap Analysis (CMMI)**

The Capability Maturity Model Integration (CMMI) is a capability improvement framework that provides guidance for organizations to elevate performance.
CMMI helps organizations benchmark their capabilities and build maturity by comparing their operations to good practices and identifying performance gaps.

**ISO/IEC 27005:2022**


**ISO/IEC 27005:2022** "Information security, cybersecurity and privacy protection provides guidance on managing information security risks" is a risk management framework applicable to all types of organizations intending to manage risks that could compromise their information security. It supports the general concepts specified in ISO/IEC 27001:2022 and is designed to assist in the implementation of information security based on a risk management approach.

## National Institute of Standards and Technology


The **NIST Cybersecurity Framework** is voluntary guidance that helps organizations, regardless of size, sector, or maturity better **understand**, **assess**, **prioritize**, and **communicate** their cybersecurity efforts**.** The Framework is not a one-size-fits-all approach to managing cybersecurity risks. The full copy of CSF 2.0 can help organizations to consider and record their own risk tolerances, priorities, threats, vulnerabilities, requirements, etc.

1. **Govern Function** – helps to establish and monitor your business's cybersecurity risk management strategy, expectations, and policy.
2. **Identify Function** – helps to determine the current cybersecurity risk to the business.
3. **Protect Function** – supports your ability to use safeguards to prevent or reduce cybersecurity risks.
4. **Detect Function** – provides outcome that help you find and analyze possible cybersecurity attacks and compromises.
5. **Respond Function** – supports your ability to take action regarding a detected cybersecurity incident.
6. **Recover Function** – involves activities to restore assets and operations that were impacted by a cybersecurity incident.

## The NIST Cybersecurity Framework:

Can be used as a top-level security management tool that aids in assessing cybersecurity risk across the organization. The framework emphasizes the importance of addressing cybersecurity risks in the organization's risk management procedures and leveraging business drivers to direct cybersecurity operations.

The **Framework Core** is a collection of industry-neutral cybersecurity practices, goals and principles. The five core functions of the framework, identify, protect, detect, respond and recover.

## NIST Risk Management Framework (NIST SP 800-37 REV.2)

The NIST Risk Management Framework (RMF) provides a flexible, holistic and repeatable seven-step process to manage security and privacy risk. It links to a suite of NIST standards and guidelines to support the implementation of risk management programs to meet the requirements of the Federal Information Security Modernization Act (FISMA).

## NIST Guide for Conducting Risk Assessments (NIST SP 800–30 REV.1)

The purpose of NIST SP 800-30 REV.1 is to provide guidance and methodology for conducting risk assessments of federal information systems and organizations. The ultimate goal is to help organizations manage the risks of IT related missions better.

## NIST SP 800-30 standard:

1. Risk assessment
2. Risk treatment
3. Risk Monitoring

**The NIST Cybersecurity Framework (CSF)** is a voluntary, risk-based framework developed by the US National Institute of Standards and Technology (NIST) to help organizations manage and mitigate cybersecurity risks. It provides a structured approach to cybersecurity risk management by outlining five key functions: Identify, Protect, Detect, Respond, and Recover

**HIPAA Compliant:**


**The Health Insurance Portability and Accountability Act of 1996 (HIPAA**) is a United States federal statute enacted by the 104th United States Congress and signed into law by President Bill Clinton on August 21, 1996. It modernized the flow of healthcare information, stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and addressed some limitations on healthcare insurance coverage.

The **HIPAA Privacy Rule** provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

**Health Insurance Portability and Accountability Act (HIPAA)** requires that employers have standard national numbers that identify them on standard transactions.


The **European Union General Data Protection Regulation (GDPR)** is the cornerstone of privacy regulations, and its impact goes well beyond the borders of the EU. Since its enforcement in May 2018, the regulation has served as the foundation for many national or state privacy regulations and acts, such as the California Consumer Privacy Act (CCPA).
GDPR impacts all organizations established in the EU or any business that collects and stores the private data of EU citizens, including U.S. organizations.

**General Data Protection Regulation (GDPR):** The General Data Protection Regulation (GDPR) is one of the most stringent privacy and security laws globally.
Tt imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching tens of millions of euros.

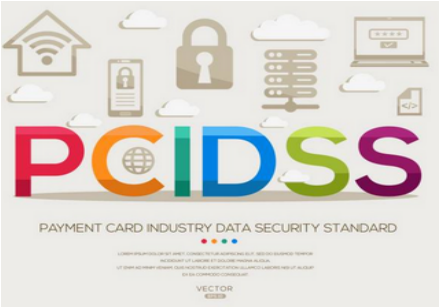
**ANSI/ISA-62443-3-2-2020 standard:**

**The ANSI/ISA-62443-3-2-2020** standard, titled "Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design," dedicates an entire section to assessing security risk for system design. The standard targets security professionals in industries mainly comprising critical infrastructure.

The **ISA/IEC 62443** standards are a comprehensive framework for securing Industrial Control Systems (ICS) and Operational Technology (OT). They address cybersecurity challenges in industrial automation and control systems by defining requirements and processes for implementing and maintaining secure systems throughout their lifecycle.

These standards set best practices for security and provide a way to assess the level of security performance.

**PCI DSS 4.0:**




The **Payment Card Industry Data Security Standard (PCI DSS)** was developed to reinforce the security of credit card transactions and facilitate the broad adoption of consistent data security measures. It provides a baseline of technical and operational requirements to protect financial data. The goal of the PCI DSS, amended to version 4.0, is to protect cardholders and sensitive authentication data wherever it is processed, stored or transmitted.

Risk assessment and management are considered best practices for maintaining compliance with PCI DSS. The standard asks organizations to "perform a risk assessment to determine the potential impact to PCI DSS scope."

The risk assessment process must identify critical assets, threats and vulnerabilities and their effects on the cardholder data environment and should result in a formal, documented analysis of risk. The PCI DSS risk assessment offers organizations guidance to help identify, analyze,

document and manage the information security risks that may affect their cardholder data. It also provides organizations with remediation strategies to implement risk management strategies that mitigate those vulnerabilities.

**Federal Information Security Modernization Act (FISMA):**

The Federal Information Security Modernization Act (FISMA) requires each federal agency to develop, document and implement an agency-wide information security program for the information and systems that support its operations and assets, including those provided or managed by a third party. The amended FISMA 2014 aims to address the evolving threat landscape, strengthen the use of continuous monitoring, and increase focus on compliance and auditing.

(FISMA, 44 U.S.C. § 3541, et seq.) is a United States federal law enacted in 2002 as Title III of the E-Government Act of 2002 (Pub.L. 107–347 (text) (pdf), 116 Stat. 2899). The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

**FISMA requires that agencies within the federal government:**

- Plan for security
- Ensure that appropriate officials are assigned security responsibilities
- Periodically review the security controls in their systems
- Authorize system processing before operations and periodically afterward

## Governance Risk and Compliance (GRC) Consultant:

1. Assess the state of the entire security program
2. Build a comprehensive security program
3. Measure maturity and conduct industry comparisons
4. Simplify communications with business leaders

**GRC Consultants have the knowledge and skills to do the following:**

1. Understand the foundations of an information Security Risk Management Program
2. Define the Scope of the Information System
3. Select and approve security and privacy controls to meet the objectives of the Risk Management Program
4. Implement the selected security and privacy controls

5. Assess the applicability and effectiveness of established security and privacy control
6. Authorize an Information System
7. Establish continuous monitoring to adapt the risk management program to the evolving risk environment.

## Footnotes:


1. Nicholas King, Risk Assessments are Essential for GDPR Compliance, July 16Th, 2019
2. **V**isit the ISACA website directly at https://www.isaca.org/standards/cobit; this is the official source for the COBIT framework, including details about COBIT 5
3. **Reference:** https://www.iso.org/standard/80585.html
4. https://csrc.nist.gov/projects/risk-management/about-rmf
5. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
6. https://doi.org/10.6028/NIST.SP.1300
7. **www.hipaajournal.com**
8. https://www.hhs.gov/hipaa/index.html
9. **General Data Protection Regulation, Link: gdpr.eu**
10. **ISA Reference,** https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
11. https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4.0
12. https://www.fedramp.gov/assets/resources/