CYBERMCBEAN
GOVERNANCE
RISK
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)

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.

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.

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:

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.

RISK ASSESSMENT:

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.

TOOLS TO MONITOR & SAFEGUARD YOUR DIGITAL ASSETS

ANTIVIRUS

FIREWALLS

ENCRYPTION

BACKUP

Several cybersecurity tools and technologies can help secure systems and networks. Firewalls, antivirus software, encryption, and intrusion detection systems are all crucial for preventing unauthorized access and mitigating risks.

DETECTION AND MONITORING 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 dentifies 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.

DETECTION AND MONITORING CAPABILITIES

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).

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.

DATA PRIVACY AND COMPLIANCE

Ensuring Data Privacy and Compliance

Data privacy laws such as GDPR and CCPA mandate strict regulations on how companies handle and store personal data. Cybersecurity helps ensure compliance by safeguarding sensitive information and avoiding costly fines due to data breaches

GDPR Compliance

Follow guidelines to protect European Union citizens' data

CCPA Regulations

Secure California residents' personal information.

Data Encryption

Encrypt sensitive data to comply with privacy laws.

Privacy Policies

Regularly update company policies to align with regulations

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.

COBIT 5 COMPLIANCE

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.

ISO/IEC 27005:2022 COMPLIANCE

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.

THE NIST CYBERSECURITY FRAMEWORK

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.

EUROPEAN UNION GENERAL DATA PROTECTION REGULATION (GDPR)

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: ISA/IEC 62443

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.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

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.”

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

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.

THANKS FOR YOUR ATTENTION!