Security Governance, Risk & Compliance (GRC) Service Definition

Purpose

To establish a structured security governance framework, manage organizational risk, and ensure continuous compliance with global regulatory and industry standards. The service enables organizations to maintain financial integrity, mitigate cyber risks, and demonstrate compliance to stakeholders, regulators, and customers.

Service Overview

CyberProof's GRC and Audit Consulting services provide expert guidance to help organizations:

- Design and implement compliance programs aligned with regulations (HIPAA, GDPR, FISMA) and standards (ISO/IEC, PCI DSS, NIST).
- Conduct risk assessments and develop mitigation strategies.
- Strengthen internal controls and governance frameworks.
- Ensure adherence to regulatory requirements and audit readiness.
- Enhance operational efficiency and security posture through continuous improvement.

Key Activities

- **Compliance Program Development** – Align programs with global standards and regulations.
- **Risk Assessment & Management** – Identify, evaluate, and mitigate security risks.
- **Internal Control Evaluation** – Perform gap analysis and strengthen controls using CIS, NIST, ISO frameworks.
- **Regulatory Compliance Review** – Ensure adherence to laws such as GDPR, CCPA, DORA, NIS2.
- **Policy & Procedure Development** – Create and maintain security policies and SOPs.
- **Audit Planning & Execution** – Conduct compliance audits and provide actionable recommendations.
- **Training & Awareness Programs** – Educate employees on compliance and risk management.
- **Governance Framework Enhancement** – Advise on board responsibilities and ethical standards.

Value Delivered

- A mature security program aligned with business objectives.
- Reduced risk exposure through proactive risk management.
- Demonstrated compliance to regulators and stakeholders.
- Improved operational efficiency and governance maturity.
- Enhanced resilience against regulatory and cyber threats.

Service Dependencies

- Access to existing policies, risk registers, and audit reports.
- Availability of IT and business process documentation.
- Stakeholder engagement for workshops and approvals.
- Access to GRC tools and platforms for integration.
- Support for control implementation and change management.

Deliverables

- Risk Assessment Reports
- Compliance Checklists & Monitoring Reports
- Gap Analysis & Audit Reports
- Governance Framework Documentation
- GRC Dashboard for real-time insights
- Audit Support Reports

Service Levels

SLAs are tailored based on engagement scope and agreed timelines. Typical SLAs include:

- Acknowledgment of requests within agreed hours.
- Delivery of compliance reports and risk assessments within project timelines.
- Regular progress reviews (weekly/monthly/quarterly).

Roles & Responsibilities

- **GRC Service Manager** – Oversees delivery and client communication.
- **Risk Analyst** – Conducts assessments and maintains risk registers.
- **Compliance Officer** – Monitors regulatory compliance and updates policies.
- **Governance Specialist** – Develops governance frameworks.
- **Audit Lead** – Plans and executes audits.
- **Data Protection Officer (DPO)** – Ensures compliance with data privacy laws.