Demystifying GRC: Who's on the Team?

A Simple Guide to Governance, Risk, and Compliance Roles

What is GRC?

Governance: How an organization is directed and controlled

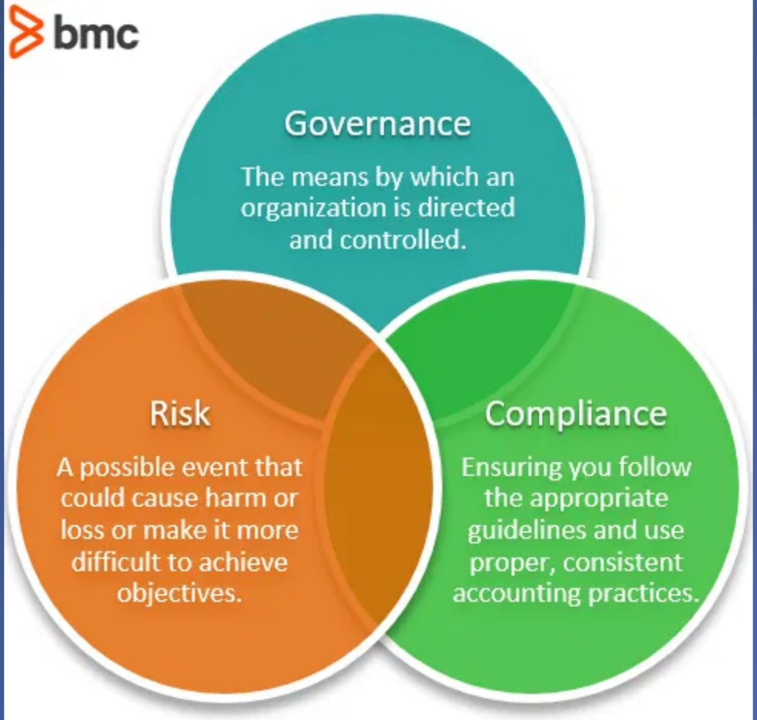
Risk: Identifying and mitigating potential threats

Compliance: Adhering to laws, regulations, and policies

Think of a sports team:

- CEO = Head Coach (sets vision)
- CISO = Defensive Coordinator (protects)
- Compliance Officer = Referee (enforces rules)
- GRC = The integrated game plan for success

✓ **Why it matters:** GRC helps organizations achieve goals, protect assets, and stay within legal boundaries.



Governance

The means by which an organization is directed and controlled.

Risk

A possible event that could cause harm or loss or make it more difficult to achieve objectives.

Compliance

Ensuring you follow the appropriate guidelines and use proper, consistent accounting practices.

The Three Lines Model: A Framework

The First Line: Owning and Managing Risk

Analogy: The Players on the Field

Frontline staff and operational managers who own and manage risk in their daily work.

The Second Line: Oversight and Expertise

Analogy: The Coaches on the Sideline

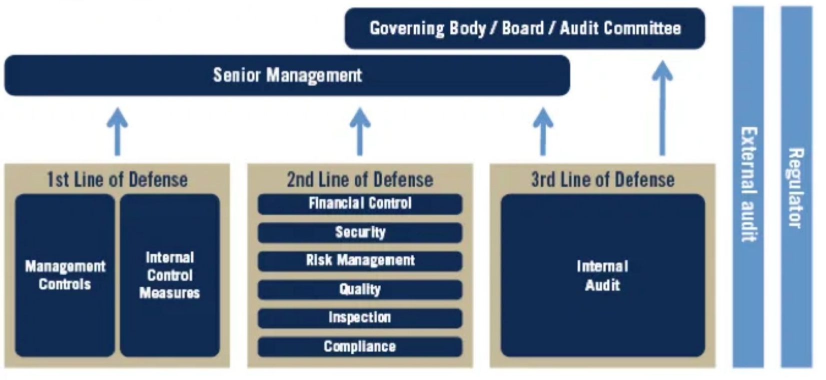
Specialized risk and compliance functions that provide expertise, set policies, and monitor the first line.

The Third Line: Independent Assurance

Analogy: The Referees and Umpires

Internal and external auditors who provide an independent check on the effectiveness of the first two lines.

The Three Lines of Defense Model



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Strategic Leadership: The Second Line (Part 1)

The Front Office and Head Coaches

♚ Board of Directors & CEO

Sets the "tone at the top" and overall GRC strategy

♞ Chief Risk Officer (CRO)

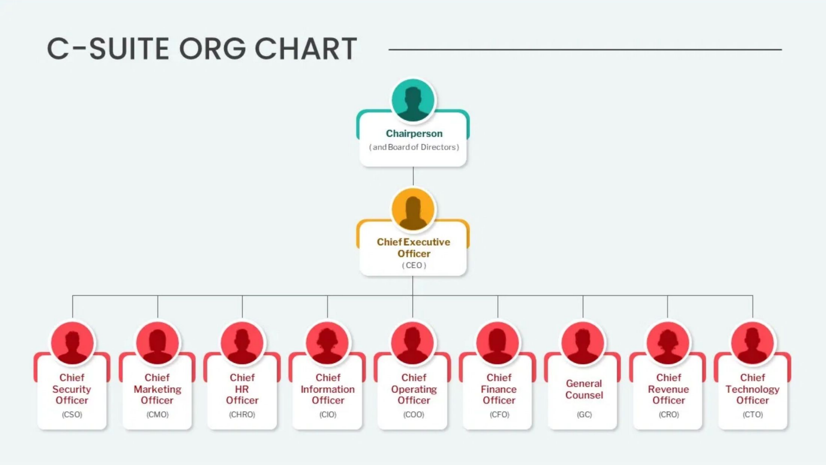
The master strategist who guides risk management initiatives

⚖ Chief Compliance Officer (CCO)

The rulebook expert ensuring adherence to laws and regulations

🛡 Chief Information Security Officer (CISO)

The defensive coordinator protecting information assets



Management and Oversight: The Second Line (Part 2)

GRC Manager / Lead

The Team Captain

Oversees day-to-day execution of the GRC program, coordinates activities across departments.

Risk Manager

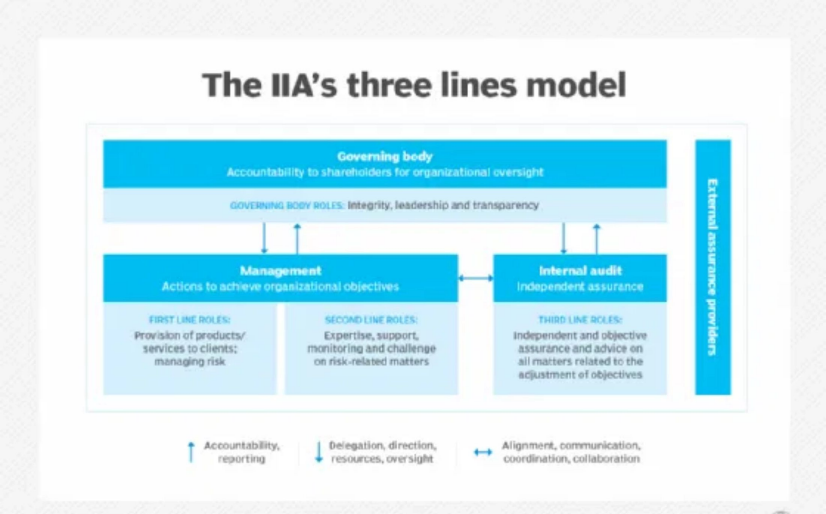
The Risk Assessor

Identifies, assesses, and prioritizes risks; maintains the organization's risk register.

Compliance Manager/Officer

The Rule Enforcer

Develops compliance programs, conducts training, monitors regulatory changes.



The IIA's three lines model

Governing body
Accountability to shareholders for organizational oversight
GOVERNING BODY ROLES: Integrity, leadership and transparency
Management
Actions to achieve organizational objectives
FIRST LINE ROLES:
Provision of products/ services to clients; managing risk
SECOND LINE ROLES:
Expertise, support, monitoring and challenge on risk-related matters
Internal audit
Independent assurance
THIRD LINE ROLES:
Independent and objective assurance and advice on all matters related to the adjustment of objectives
External assurance providers
↑ Accountability, reporting
↓ Delegation, direction, resources, oversight
↔ Alignment, communication, coordination, collaboration

Frontline Implementers: The First Line

The Players on the Field

GRC, Risk, and Compliance Analysts

The Doers and Documenters

Perform risk analysis, test controls, document findings, and monitor compliance status using specialized software.

IT and Security Teams

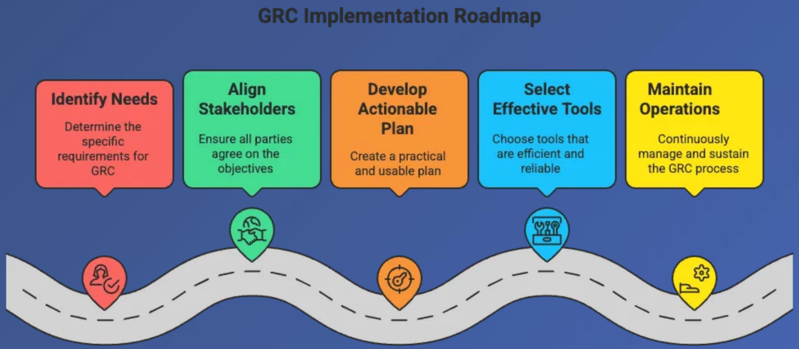
The Technical Crew

Build, implement, and maintain technical security controls that protect the organization's digital infrastructure.

Control Owners

The Departmental Specialists

Execute and maintain specific GRC controls within their areas of expertise (HR, Finance, Operations, etc.).


GRC Implementation Roadmap
Identify Needs
Determine the specific requirements for GRC
Align Stakeholders
Ensure all parties agree on the objectives
Develop Actionable Plan
Create a practical and usable plan
Select Effective Tools
Choose tools that are efficient and reliable
Maintain Operations
Continuously manage and sustain the GRC process

Independent Assurance: The Third Line

Internal Auditor Role

Tests the effectiveness of GRC controls and processes implemented by the first and second lines.

Reports findings directly to senior leadership and the Board of Directors.

Provides an unbiased view of the program's health and ensures accountability.

Why Independence Matters

Free from influence of the teams they evaluate

Ensures objective assessment without conflicts of interest

Creates trust in the overall GRC framework

Important Distinction: Unlike Compliance Officers (who ensure adherence to external laws), Internal Auditors focus on independently testing the effectiveness of internal controls and processes.

Internal Auditor (IA)

[in-ˈtər-nᵊl ˈȯ-də-tər]

A trained professional employed by companies to provide independent and objective evaluations of financial and operational business activities, including corporate governance.

Investopedia

GRC Career Paths: Beyond the Job Title

Important Note: "GRC" is often a concept describing how different functions intertwine, rather than a specific job title.

Risk Management

- Risk Analyst
- Risk Manager
- Enterprise Risk Director

Compliance

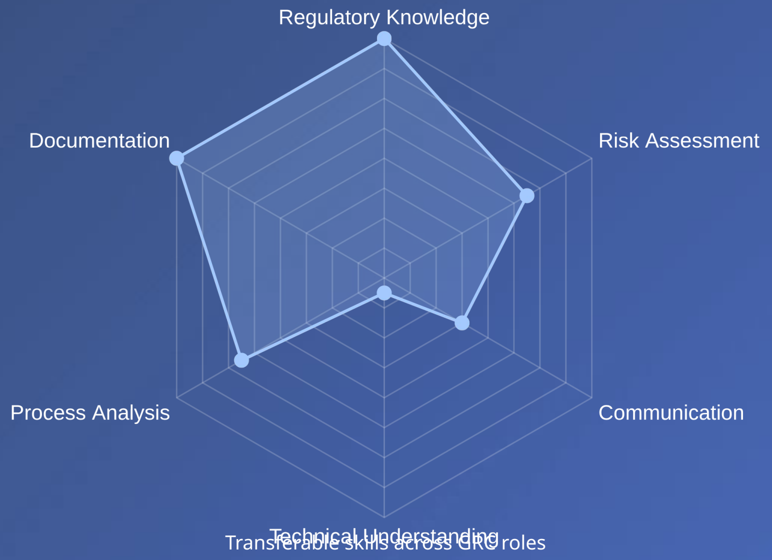
- Compliance Analyst
- Compliance Officer
- Chief Compliance Officer

Audit & Assurance

- Security Auditor
- Internal Auditor
- IT Audit Manager

Security & IT

- Information Assurance
- ISSO/ISSM
- Third-Party Risk Analyst



Why GRC Matters: Real-World Impact

Protection

Safeguards against financial losses, legal penalties, data breaches, and reputational damage.

Trust Building

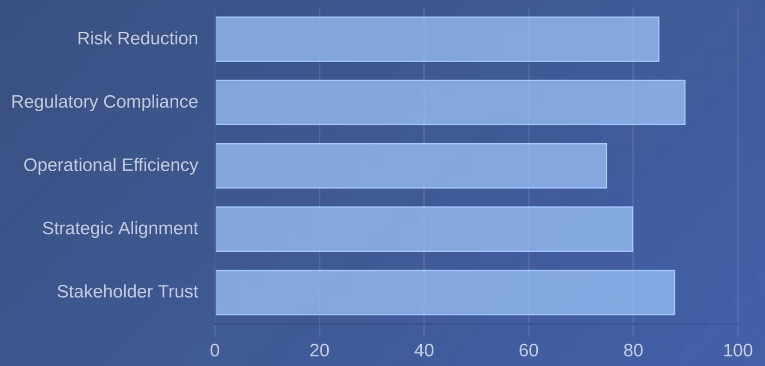
Maintains confidence of customers, investors, regulators, and other key stakeholders.

Enabling Innovation

Creates a stable foundation that empowers the organization to take calculated risks and grow with confidence.

Strategic Decision-Making

Enables risk-informed decisions that align with business goals and build organizational resilience.



Key Benefits of Effective GRC Implementation

Key Takeaways

- GRC is a team effort with distinct roles working together toward common goals
- The Three Lines Model provides a clear framework for understanding responsibilities
- Strategic leadership sets the tone, while frontline staff implement controls
- Effective GRC protects organizations and enables innovation through risk management
- Independence in the Third Line ensures objective assessment and accountability

Further Learning

IIA Three Lines Model

Comprehensive framework for organizational governance

ISACA GRC Professional Certification

Industry-recognized credential for GRC professionals

OCEG GRC Capability Model

Open standard for integrating governance, risk, and compliance

Questions? Contact us at grc@example.com