GRC 101—an Introduction to Governance, Risk Management, and Compliance

capgemini.com/2017/10/grc-101-an-introduction-to-governance-risk-management-and-compliance

October 24, 2017

The acronym "GRC" stands for governance, risk management, and compliance. But what is the scope of GRC and what are its boundaries? Is it a technology, a tool or a process? Does GRC refer to the platform? Should your organization maintain a separate GRC department? In this blog, I provide an introduction into what GRC is, answering key questions on where it acts and why it's important.

What is GRC?

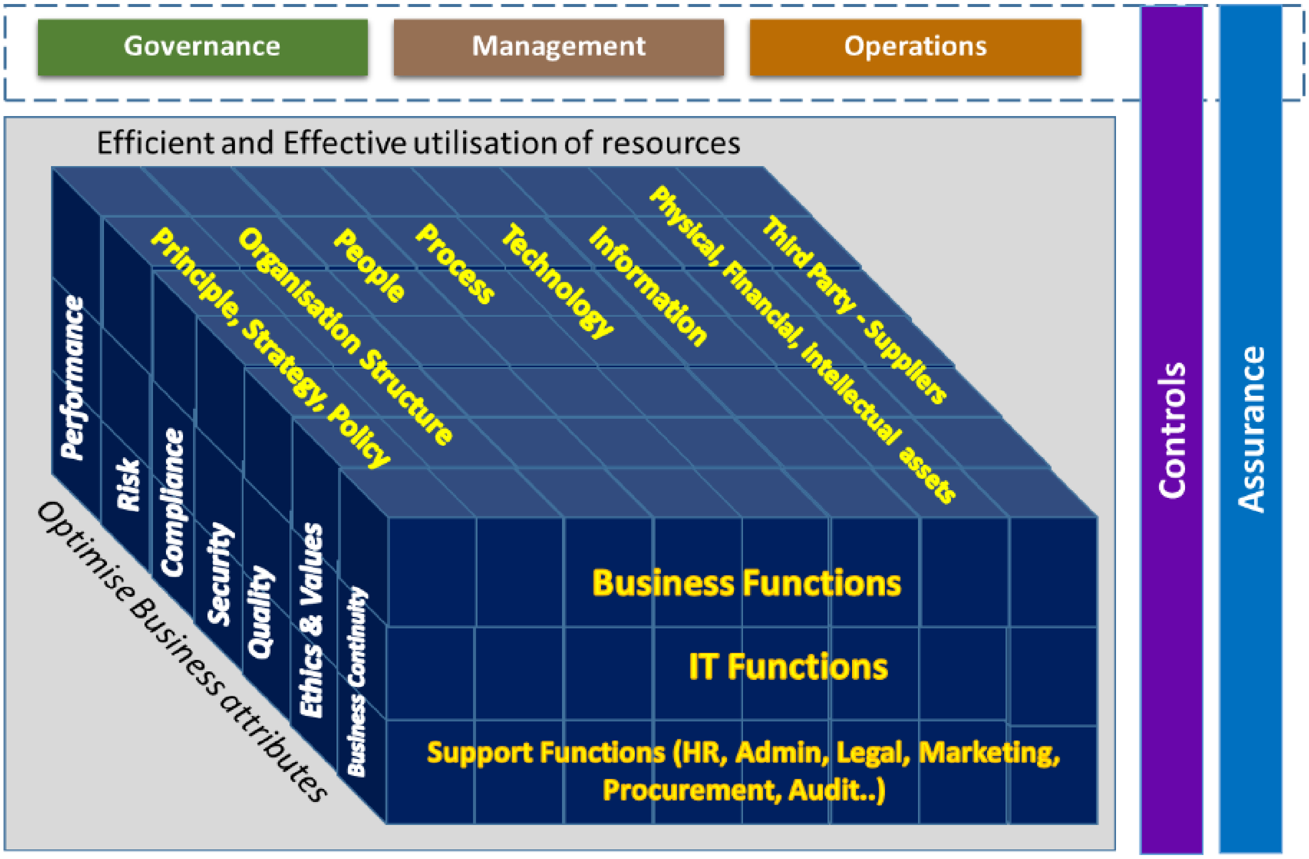
Many people think of a platform when referring to GRC. But GRC refers to a capability that helps an organization achieve its objectives, with responsibility running right across the organization. GRC is a set of processes and practices that runs across departments and functions. GRC might be enabled by a dedicated platform and other tools, although this is not mandatory. While organizations generally don't need to maintain a separate GRC department, most organizations have a team in place to manage the GRC platform and tools.

What is the scope of GRC?

By definition, the scope of GRC doesn't end with just governance, risk, and compliance management, but also includes assurance and performance management. In practice, however, the scope of a GRC framework is further getting extended to information security management, quality management, ethics and values management, and business continuity management.

In order to get a better understanding of GRC, we first need to understand the different dimensions of a business:

The dimensions of a business

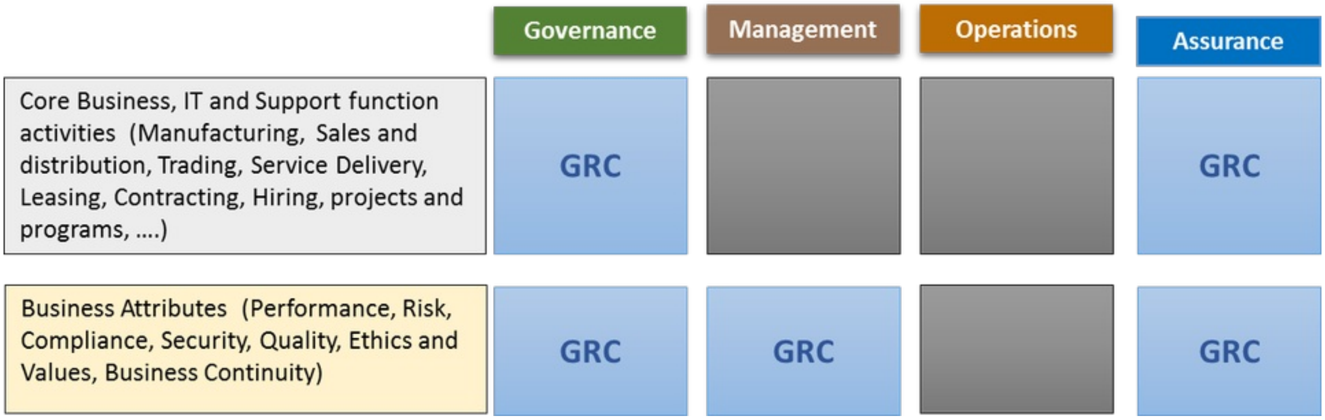


Business, IT and support functions—an enterprise will have business, IT and support functions such as finance, HR, administration, legal, marketing, procurement, audit, etc.

- **Resources**—required to conduct business, including strategies, policies, standards, procedures, organizational structure, roles and responsibilities, people, processes, technology, information, physical, financial and intellectual assets, and third parties (suppliers, vendors and contract employees).
- **Business attributes**—the key attributes of a business include:
- Performance, including goals, targets, outcomes, profitability and SLAs, etc.
- Risk, including financial risk, credit risk, market risk, strategy risk, operational risk, fraud risk, reputational risk, information security risk, technology risk and compliance risk, etc.
- Compliance, including regulatory compliance (SOX, PCI/DSS, GDPR), legal compliance (labor laws), organizational compliance (policies and standards), security (human, physical and information security), quality, ethics and values.
- **Governance, management, and operations**—governance involves setting directions, optimizing risks and resources, and monitoring performance and compliance to achieve an organization’s objectives. It can be broadly classified into corporate governance, business governance, IT governance and legal governance. Management involves planning, organizing, leading, coordinating, controlling and reporting. Operations includes executing the process and function.

- **Controls**—in order to realize value from the business, resources should be utilized efficiently and effectively, and business attributes should optimized. This is only possible when appropriate controls are implemented and executed. The controls can be classified as management controls, process controls, technical controls and physical controls. Controls are applied to the resources as well as the attributes.
- **Assurance**—independent assurance is required to ensure that controls are designed and operating effectively, and compliance requirements are met consistently. It is the responsibility of governance to monitor and obtain assurance. Assurance will be primarily through audits. There are several types of audits. Internal and external audits, certification audits, financial audits, IT audits, compliance audits, process audits and security audits, etc.

The scope of GRC based on the definition and current trends



	Governance	Management	Operations	Assurance
Core Business, IT and Support function activities (Manufacturing, Sales and distribution, Trading, Service Delivery, Leasing, Contracting, Hiring, projects and programs, ….)	GRC	▨	▨	GRC
Business Attributes (Performance, Risk, Compliance, Security, Quality, Ethics and Values, Business Continuity)	GRC	GRC	▨	GRC

Why is GRC important?

Effective GRC implementation helps the organization to reduce risk and improve control effectiveness, security and compliance through an integrated and unified approach that reduces the ill effects of organizational silos and redundancies.