WHAT IS GRC? GOVERNANCE, RISK, AND COMPLIANCE EXPLAINED

Any organization seeking to meet its business objectives continues to face a myriad of challenges owing to the ever-changing complexity of the business environment:

- Regulation (e.g. SOX, HIPAA, GDPR, PCI-DSS,)
- People (diversity, millennials, skills gap, etc.)
- Technology (IoT, AI)
- Processes
- Many more aspects

For this reason, there is an increasing need for enterprises to put in place mechanics to ensure that the business can successfully ride the wave of these complexities. GRC—Governance, Risk, and Compliance—is one of the most important elements any organization must put in place to achieve its strategic objectives and meet the needs of stakeholders.

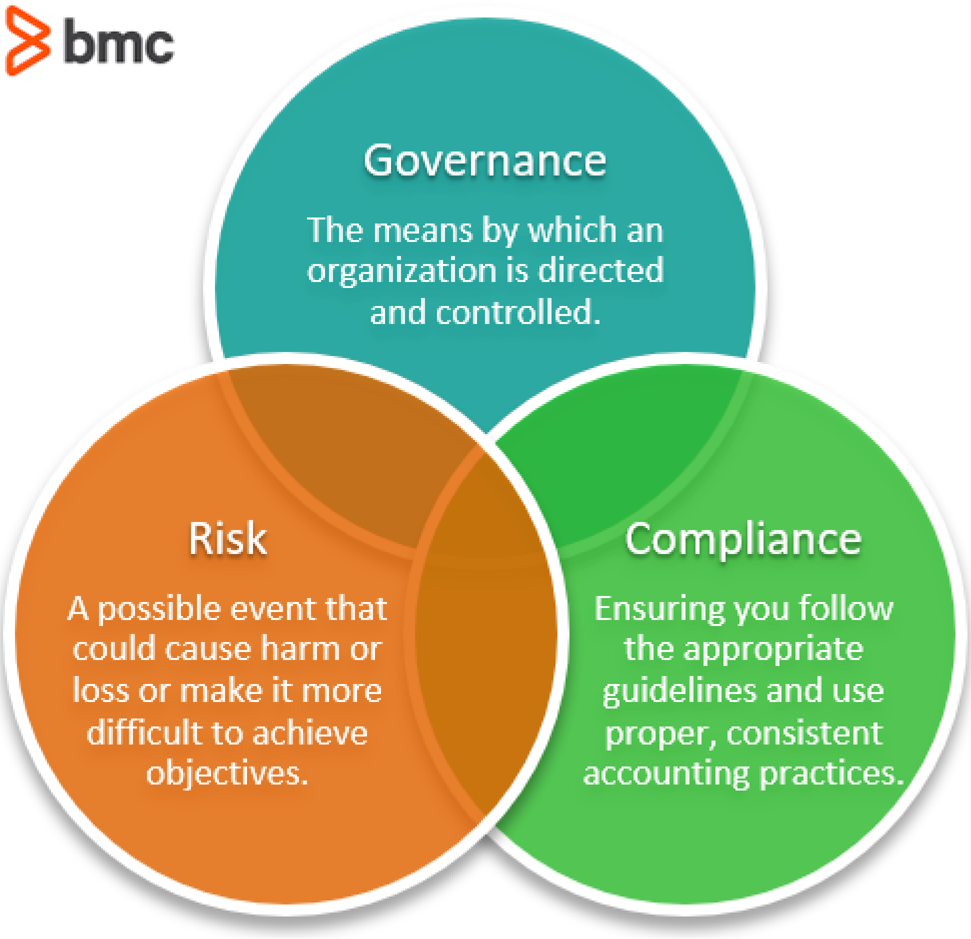
What is GRC?

GRC as an acronym stands for governance, risk, and compliance, but the term GRC means much more than that. The OCEG (formerly known as "Open Compliance and Ethics Group") states that the term GRC was first referenced as early as 2003, but was mentioned in a peer reviewed paper by their co-founder in 2007.

The OCEG views GRC as a well-coordinated and integrated collection of all the capabilities necessary to support principled performance at every level of the organization. These capabilities include:

- The work done by internal audit, compliance, risk, legal, finance, IT, HR
- The work done by the lines of business, the executive suite, and the board itself
- The outsourced work done by other parties and carried out by external stakeholders

Principled Performance refers to a point of view and approach to business that helps organizations reliably achieve objectives while addressing uncertainty and acting with integrity.


bmc
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.

When broken down, the constituent elements can be defined from ITIL® 4 and explained as follows:

Governance

The means by which an organization is directed and controlled. In GRC, governance is necessary for setting direction (through strategy and policy), monitoring performance and controls, and evaluating outcomes.

Risk

A possible event that could cause harm or loss or make it more difficult to achieve objectives. In GRC, risk management ensures that the organization identifies, analyses, and controls risk that can derail the achievement of strategic objectives.

Compliance

The act of ensuring that a standard or set of guidelines is followed, or that proper, consistent accounting or other practices are being employed. In GRC, compliance ensures that depending on the context, the organization takes measures and implements controls to assure that compliance requirements are met consistently.

Drivers for GRC

Without a doubt, the biggest driver for GRC is regulation. While traditional industries such as banking, insurance, healthcare, and telecoms have borne the brunt of regulation in the past, today's digital age is fueling a risk in regulation that touches all entities, large or small.

Use of data, particularly personally identifiable information, has huge business potential as well as risk of abuse. Therefore, governments and international agencies are paying a closer eye to how digital businesses manage data. The rise in cyber-attacks, which expose personal data, as well as growing awareness by individuals and civil rights organizations have shed new light into how companies manage information and technology through processes, people, and culture.

Benefits of GRC framework

According to CIO.com, benefits of GRC include:

- Improved decision-making
- More optimal IT investments
- Elimination of silos
- Reduced fragmentation among divisions and departments

A collective approach is the best bet for any organization seeking to get to grips with the ever-changing regulatory landscape. When GRC is done right across the whole organization, and the right people get the right information at the right time, and the right objectives and controls are established, then OCEG states that we can expect reduction in costs, duplication, and impacted operations.

The organization can also benefit through better decision-making agility and confidence, as well as sustained, reliable performance, and delivery of value.

The GRC approach

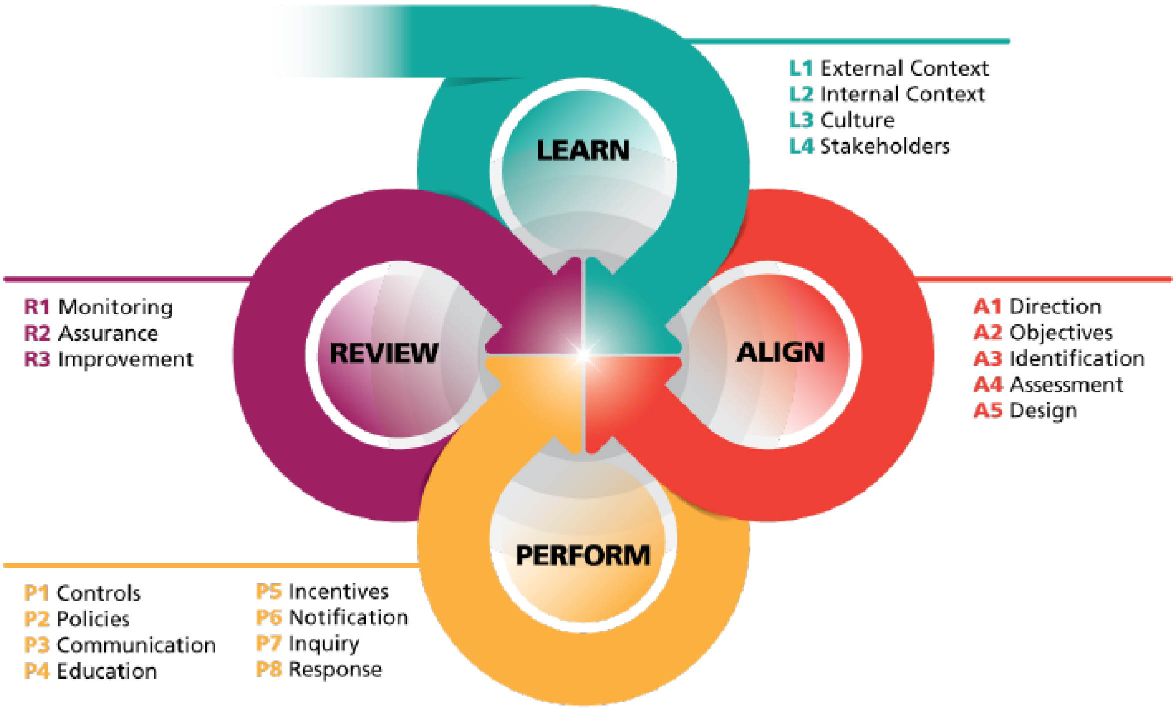
As has been stated before, GRC is best implemented in a holistic manner that encompasses the entire organization. This does not necessarily mean that an umbrella unit is required for coordination, even though that might work for certain types of entities. The OCEG has defined an open source approach called the GRC Capability Model (also called the Red Book) that integrates the various sub-disciplines of governance, risk, audit, compliance, ethics/culture and IT into a unified approach. The Capability Model is made up of four components:

- **LEARN** about the organization context, culture and key stakeholders to inform objectives, strategy and actions.
- **ALIGN** strategy with objectives, and actions with strategy, by using effective decision-making

that addresses values, opportunities, threats and requirements.
- **PERFORM** actions that promote and reward things that are desirable, prevent and remediate things that are undesirable, and detect when something happens as soon as possible.
- **REVIEW** the design and operating effectiveness of the strategy and actions, as well as the ongoing appropriateness of objectives to improve the organization.

These components outline an iterative continuous improvement process to achieve principled performance and are further decomposed into elements which are then supported by practices, actions and controls. The actions and controls are classified in three types, which organizations can select a mix depending on their context:

- Proactive
- Detective
- Responsive



GRC Capability Model - Element View (Source: OCEG Red Book)

GRC use cases

Organizations use GRC to integrate processes and tools to manage risks, meet compliance demands, and serve their own objectives. Here are typical examples of uses:

- **Establishing Policies and Practices**
  - A GRC framework helps organizations establish policies and practices to minimize compliance risk.
  - IT and security GRC solutions leverage timely information on data, infrastructure, and applications (virtual, mobile, cloud).
- **Improving Efficiency**
  - Centralizing issues into one framework eliminates duplicate efforts.
  - GRC creates a "single source of truth" to provide consistent and up-to-date information to everyone.

- **Streamlining GRC Activities**
  - Monitoring compliance, risks, and governance can be automated to reduce manual work.
  - Many tasks can be systematized to save time and reduce errors.
- **Managing Financial and AI-Driven Models**
  - GRC guides model development, validation, and use.
  - It makes it easier to catalog and manage all models in use.
  - GRC ensures models are in compliance with applicable regulations.
  - GRC provides guidelines and standards for how organizations can use AI ethically.
- **Risk Assessment and Reduction**
  - Organizations can get ahead with prevention, using the framework to identify risks.
  - GRC facilitates creating scenarios to analyze and formulating proactive protections to prevent problems.
- **Support for Companies with Compliance Failures**
  - GRC can help organizations track and analyze incidents to identify root causes, and provides an audit trail.
  - The framework helps with impact assessments, incident response, and corrective actions.
  - GRC provides support in case of future failures.
- **Improving Compliance**
  - GRC helps organizations identify areas where they are non-compliant and vulnerable.
  - It supports proactive reporting.
  - GRC contributes to creating a culture of compliance.
- **Better Policies and Management**
  - Organizations can standardize their policies and apply them consistently.
  - It is easier to respond to regulatory changes quickly, even automatically.
  - Companies can make faster, more informed decisions.

GRC solutions

In order to address the needs of GRC, a lot of organizations are turning to technology solutions. These solutions enable the leadership to monitor GRC across the enterprise by ensuring business processes and information technology continue to align to the governance, risk and compliance requirements of the organization. Capabilities include:

- Risk management (logging, analysis, and management)
- Document management
- Audit management
- Reporting
- Analytics

However, having a GRC tool alone isn’t enough to guarantee effective GRC. Technology doesn’t have ethics—people do. Hence GRC must be addressed from a people and process perspective, even before technology is considered.

However, technology is a very good enabler in reducing the “compliance” overhead that comes with gathering and managing records required to prove that the organization is meeting GRC requirements, without overburdening employees who should be focused on generating value instead.

Challenges of implementing GRC systems

Despite the many advantages, implementing GRC systems can be difficult for some organizations. To smooth adoption and get full value from the framework, consider how to address issues such as:

- **Change Management**
  - Though GRC supports making good decisions in a business environment that is changing quickly, some organizations resist change or lack the agility to act in response to new insights.
- **Data Management**
  - GRC makes it possible to break down data silos, so that data from any part of the organization can be shared across the organization. However, eliminating duplicate data and dealing with data management issues are very real challenges.
- **Lack of a Comprehensive GRC Framework**
  - Some organizations struggle to seamlessly integrate GRC across business activities, leading to a fragmented GRC framework.
- **Ethical Culture Development**
  - The collaborative nature of GRC and the need for sharing and transparency can challenge the status quo of some organizations. Clear leadership and recognition for ethical behavior are keys to establishing a new culture.
- **Inadequate Technology and Other Resources**
  - Legacy IT systems may not have the flexibility or the potential to scale, slowing adoption and creating more manual work.
  - Implementation requires an investment of time, talent, and money, which may not be possible in some organizations.
- **Insufficient Training**
  - Your organization may not have personnel skilled across GRC implementation and issues. The result can lead to resistance to adopting GRC and poor implementation.

Additional resources

Explore more on this topic with the BMC Security & Compliance Blog and our Guide to Security & Compliance.