WHITE PAPER | ComplyWorks

COMPLYWORKS

What is GRC?

What is GRC and where did it come from?

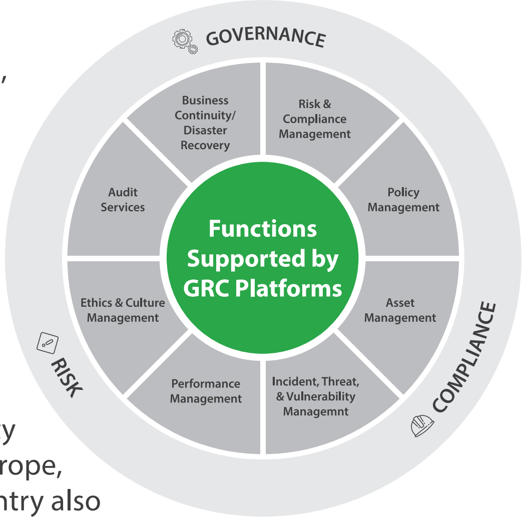
At a glance:

***Governance** – is how senior leaders and the board of directors, oversee and manage the entire organization. They use risk and compliance information to mitigate, manage or avoid risks.*

***Risk Management** – the processes used to identify, review and respond to risks that could impact the organization or prevent it from achieving its business objectives.*

***Compliance** – is the consistency in which an organization adheres to defined laws, regulations and standards.*

The acronym “GRC" stands for governance, risk management and compliance. It came into being after several highly publicized, corporate financial, environmental and safety disasters, after which governments and independent regulators imposed stringent GRC requirements on organizations. While this is not a new change, many organizations are still struggling to improve their internal processes to better manage risk and prevent business and compliance failures.


GOVERNANCE
Business Continuity/ Disaster Recovery
Risk & Compliance Management
Audit Services
Policy Management
Functions Supported by GRC Platforms
Ethics & Culture Management
Asset Management
Performance Management
Incident, Threat, & Vulnerability Managemnt
RISK
COMPLIANCE

As organizations adopt new business models, deploy new technologies and establish operations in other countries, they must determine the strategic impact of these changes on their organization and modify their governance, risk management and compliance priorities to suit.

Why should I care about GRC?

Organizations are facing increased complexity and unprecedented regulatory change. In Europe, despite many harmonized policies, each country also has its own laws and regulations. In addition, many Asian and North American countries have increased regulations in the last few years. This increase in legislation creates complexity in managing GRC requirements across countries, which can increase demands placed upon organizations.

In reaction to the increase in regulatory demands, many organizations have chosen to outsource their operations and regulatory burdens to third-parties to achieve significant cost savings. However, many employers miss the mark when establishing proper GRC controls between themselves and their third-party contractors which further exposes the organization. Governments have made it clear that while organizations can outsource the work, they cannot outsource the liability.

Increasingly, the board of directors is being held accountable for GRC non-compliance and for issues that it may not be very knowledgeable on. Regulators and governments have made it clear that an organization’s operations are not only the responsibility of senior executives but also the board of directors. Misconduct or negligence by board members and the executive can result in fines, lawsuits and even jail time if found guilty.

What is GRC?

What is an integrated GRC program and what are the benefits?

Surveys conducted by Ernst and Young have found that organizations with embedded risk management practices outperform their peers.

Top-performing organizations implement on average twice as many risk management programs as those in the lowest-performing group.

The top 20 percent of these top performing organizations generated ***three times the level*** *of earnings as those in the bottom 20 percent.*

Despite the risks, many organizations do the bare minimum to meet regulatory requirements and this does not always have the intended effect of addressing its full scope of risk. Organizations can still experience GRC breaches, incidents or reputational impacts even though they have passed the bare minimum regulatory standards. One way to manage these increasing demands is through an integrated GRC program that is embedded in the organizational culture.

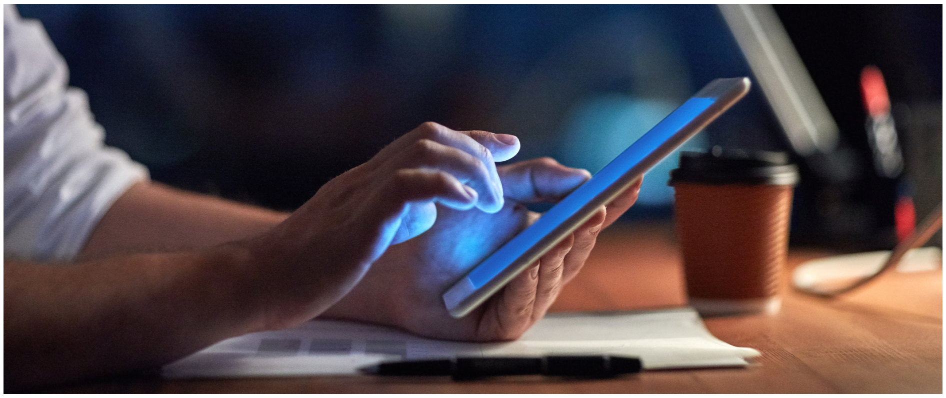
An integrated GRC program is a program that spans all departments of an organization and is ingrained into the organization's operations and culture. The most obvious benefits to an integrated program are streamlined data collection and the ability to quickly generate reports in one centralized platform. An integrated GRC program also helps organizations be flexible in constantly changing environments, mitigate business risk and prevent financial and material loss.

Some of the main goals of implementing an integrated GRC program are to:

1. **Establish long-term best practice protocols**
2. **Improve decision-making agility**
3. **Enable better capital allocation to the right initiatives at the right time**

These goals help to create a consistent corporate management culture, highlight inherent strategic, operational and regulatory risks and drive top to bottom accountability for key GRC objectives.

The benefits are clear. Instead of risk management being a cost burden, the research shows that there is a significant financial incentive for organizations to prioritize risk management and implement it into daily operations.



What is GRC?

What are some of the barriers to success?

A recent global EY survey found that only:

***49%** of organizations said they use some type of technology solution for risk management activities*

***29%** of organizations said they review risk dashboards/metrics on a monthly basis*

This shows that while our world continues to focus more on technology, organizations can be slow to adopt new solutions, even if the technology can increase visibility into the GRC program.

Some GRC programs are comprehensive and well thought-out in terms of strategy, processes and technology, but they ignore the human dynamic. For an effective GRC program to succeed, it needs an influential executive champion who can lead the program and help drive change. Failure to find a strong leader to drive the program forward can easily derail the initiative, no matter how well planned it may be.

Unifying risk initiatives and programs across an organization is a massive effort. Many organizations develop silos, which often duplicate personnel, processes and technologies, and prevent leaders from obtaining a clear view of the organization's risk landscape. This, in turn, limits organizations from effectively managing risk, while wasting time, money and resources.

Some of the most common pitfalls to implementing a successful GRC program include:

1. **Lack of transparency**
   Implementing a new GRC program in secrecy will limit employee adoption. The GRC team must clearly outline the new expectations and policy measures, the key indicators of success and the overall end goal.

2. **Continued investment in legacy technology**
   Many organizations fail to recognize the deficiencies of their home-grown systems (e.g. lack of integration or the inability to centrally store documents and records). Others manage their GRC program manually across disparate functional groups and geographies. Organizations need to ensure that the technology solution they select will empower the GRC program team, meet the demands of a growing business and is able to support both internal staff and third-party contractors, vendors and suppliers.

3. **Lack of program updates**
   A GRC program needs to be continually updated to stay current with regulations and must adopt regular program reviews, audits and program enhancements. This is where many GRC programs begin to fail.

What is GRC?

What are the best practices?

GRC is not a one-and-done process. Instead, it is an organization-wide program with multiple processes that need to be continuously improved. There are many GRC models that organizations can follow. Some of the more common GRC models from prominent GRC reference organizations include the Committee of Sponsoring Organizations (COSO), the GRC Capability Model (OCEG) and the International Standards Organization (ISO 19600).

Some of the best practices to implement an effective GRC program are to:

Review the organizational risk environment – conduct an analysis of all costs related to GRC activities for their internal and contingent workforce. Next, research and identify where there are existing gaps, overlaps or key areas of risk that need to be addressed. Finally, define the program's objectives and key indicators of success to ensure program transparency.

Empower the GRC program with integration – by supporting an integrated GRC program with representation from across the organization, teams can ensure that the program is consistently deployed organization-wide while allowing for local variances. It enables organizations to break down silos, streamline reporting and provide clear oversight to senior leadership.

Define and implement a risk-based "threshold" approach – define acceptable risk thresholds and implement them consistently across the organization. A key part of this is requiring all employees to undergo risk-related training and formalize acceptance of any policies/the GRC program. It is also important to embed GRC practices into business planning and employee performance reviews to ensure adoption and accountability.

Improve transparency – leading GRC organizations consistently communicate with stakeholders to ensure they are kept up-to-date. This creates accountability, especially if the communication has a sign-off requirement.

Standardize risk monitoring and reporting – it is important for organizations to build their GRC programs with clear objectives, indicators of success and established processes for regular monitoring and reporting.

Even with the use of these best practices, many organizations struggle with the adoption of new GRC programs because it is seen as additional work by employees. Fortunately, technology has created the opportunity for many efficiencies with new GRC programs, reducing duplication, improving risk management and ensuring that the right projects get funded at the right time.

What is GRC?

The power of technology and ComplyWorks

Historically, understanding GRC regulations for each country, state or province would require the help of many teams of full-time employees. This consumed a lot of resources as employees would have to manually collect and organize a significant amount of data, leaving little time left for reporting and analysis. With new technology and an increasingly connected world, technology is now empowering teams in new ways to overcome the challenges of the old manual-based methods.

Web-based solutions like ComplyWorks' Compliance Management System (CMS) can make it much easier to manage a GRC program. Our CMS allows organizations to manage their HSE and GRC programs by addressing the area of highest risk – management of third-party contractors. By working closely with our clients, we can help them gather the information most relevant to them. This allows organizations to have a constant view on their areas of risk to improve operations and provide oversight to senior leaders.

ComplyWorks' compliance management platform covers the entire GRC lifecycle – from basic prequalification to managing your third-party workforce at worksites locally, regionally or globally. We make GRC easy and achievable with our web-based integrated solutions.

ComplyWorks CMS solution can support a robust GRC program with:

- A centralized platform that enables decentralized decision making.
- Multiple department access with client designed user permissions.
- Facilitation of GRC training with knowledge retention.
- Invites and formalization of policy acceptance, procedures and overall program understanding.
- Storage capabilities to house the latest GRC documents, policies and procedures.
- Dynamic reporting and monitoring dashboard that alerts for non-compliance.
- Ongoing GRC communication transparency.
- The improvement of health, safety and environmental (HSE) outcomes.
- Increased end-user adoption, easy to use navigation and action driven dashboards.

See how ComplyWorks can reduce your risk with a free solution demo. It may be the best decision you make today.

Sources:

1. A process model for integrated IT governance, risk, and compliance management; Nicolas Racz, Edgar Weippl, Andreas Seufert
2. GRC, 2012 Haymarket Media, Inc.
3. Governance, Risk and Compliance, Deloitte, Sarah Adams, Carlos Ruiz, Elias Rivera
4. Analysing The Governance, Risk And Compliance (GRC) Implementation Process: Primary Insights, Konstantina Spanaki and Anastasia Papazafeiropoulou
5. A Frame of Reference for Research of Integrated Governance, Risk and Compliance (GRC), Nicolas Racz, Edgar Weippl, Andreas Seufert
6. Exploring Strategic Risk, Deloitte
7. GRC Strategy Services, Ernst &Young
8. GRC Lessons Learned: Suggestions for Deployments, ISACA – San Francisco Chapter
9. Governance, Risk, and Compliance (GRC) White Paper, Secure Digital Solutions
10. The Human Side of GRC: The Essence of Governance, Risk and Compliance, Crisis Management International, Bruce T. Blythe and Rick J. Machold
11. Managing Governance, Risk and Compliance with ECM and BPM, The Global Community of Information Professionals, AIIM
12. Centralized operations - The future of operating models for Risk, Control and Compliance functions, Ernst &Young
13. How Mature is Your Risk Management, Michael Herrinton
14. EMR Diplomacy, Lawrence Richter Quinn
15. https://www.ey.com/Publication/vwLUAssets/Ey-global-governance-risk-compliance-survey/$FILE/Ey-global-governance-risk-compliance-survey.pdf