What is Governance, Risk Management, and Compliance (GRC)?

Governance, risk, and compliance is a strategy for managing your organization's overall governance, enterprise risk management, and compliance with regulations.

GRC is a structured approach to aligning your business objectives, while also effectively managing risk and meeting your compliance requirements.

Governance is ensuring that all organizational activities such as managing your IT operations are aligned to support your organization's business goals.

Risk is making sure that any risk or opportunity associated with your organization's activities is identified and addressed in such a way that supports your business goals.

In the context of IT, this means having a comprehensive IT risk management process that is part of your company's Enterprise risk management function.

Compliance involves making sure that organizational activities are operated in a way that meets all regulations and laws impacting the systems.

Where IT is concerned this means that making sure your IT systems and the data inside those systems are properly secured and used correctly.

Meeting compliance involves applying IT controls and auditing those controls to ensure their working as intended.

Companies also use controls to manage risks they have identified. The term "GRC" was first used in the early 2000s after many highly publicized corporate financial disasters.

As a result, enterprises scrambled to improve their internal control and governance processes.

How GRC Works

Your organization must develop a GRC framework for the organization, operation, and leadership of your company IT areas to ensure they support and enable your company's strategic objectives.

Many companies consult a framework for guidance in developing and refining their GRC functions rather than trying to create one from scratch.

These Frameworks and standards provide a basic structure that organizations can then tailor to their environment.

The major players across a number of industries are COBIT, ITIL, and COSO.

> *Though there are many wonderful software solutions to help you streamline GRC operations in your company, GRC itself is more than a collection of software and tools. It involves work done by multiple departments within a company such as legal, finance, IT, HR, compliance, risk, internal audit, the executive suite, and the board of directors.*

The Key to Successful GRC Implementation

Unless your company's C-suite executives support making a cultural change, the

decision-making, Resource Management, risk management, and Regulatory Compliance functions that are part of a GRC framework won't be effective.

Before you get started with GRC, is wise to address the issues with your company's executives providing data and research to support investing in the initiative.

What Organizations Use GRC?

Any organization, large or small, public or private can Implement GRC.

If your company wants to manage risk effectively, maintain compliance, and a line I see activities to business goals, GRC is a wonderful investment to make.

According to Joanna Grama, director of cyber-security in it GRC programs for EDUCAUSE, "We are seeing a big push in higher education to implement GRC frameworks, not necessarily to meet a revenue goal, but to ensure that institutional missions of teaching, research, outreach and student success are met efficiently and effectively."

Top GRC Certifications

Many job roles require or benefit from a GRC certification including IT security analyst, security engineer or architect, CIO, senior IT auditor, and more.

Professionals who hold GRC certifications need to balance stakeholder expectations with business objectives and ensure that the company's objectives are met while simultaneously meeting industry compliance requirements.

That's a lot of responsibility but it is absolutely necessary to running a successful business today.

GRC certification options include:

- Certified in Risk and Information Systems Control (CRISC)
- Certified in the Governance of Enterprise IT (CGEIT)
- Project Management Institute – Risk Management Professional (PMI-RMP)
- ITIL Expert

- Certification in Risk Management Assurance (CRMA)
- GRC Professional (GRCP)

If you are interested in having any of your IT staff become GRC certified, learn about each of the certification options before choosing any of them.

What GRC Solutions are Available?

It GRC Solutions enable you to develop and coordinate controls and policies and connect them to internal and regulatory compliance requirements.

These Solutions are typically cloud-based and automate many processes to increase efficiency and reduce complexity.

Some of the most popular GRC Solutions on the market include IBM OpenPages GRC platform, Rsam's Enterprise GRC, and MetricStream.

These are among some of the more expensive options on the market though affordable and free solutions are available for startups and smaller businesses that lack the budget to invest in more expensive options.

Be mindful of the fact that the lower-priced options generally lack in features compared to the higher-priced competition.

Before you begin investigating any software solution it is necessary to prepare your environment.

First, assess your organization's risk and examine controls. Are there currently adequate controls in place? are your existing controls working?

Fix any controls that aren't working as intended and add additional controls where they are needed.

You also need to create your GRC framework.

Though GRC tends to focus mostly on it, implementing a strategy encompasses the entire company and requires a deep dive into all of the people and processes that will be affected.

Why Implement GRC in Your Organization

Today's business climate is challenging. Government agencies, nonprofits, and small businesses are facing issues that only large companies had to deal with in the past.

You must deal with the fact that stakeholders demand high performance and high levels of transparency along with the fact that regulations and enforcement are constantly changing and are unpredictable.

The cost of addressing risks and requirements is quickly spinning out of control.

Growing third-party relationships and managing their risk is a major challenge. And of course, there is a major impact to the business when threats and opportunities are not identified.

Many times, organizations develop departments and programs to address these issues such as compliance, Corporate social responsibility, risk management and Performance Management.

The drawback is these departments and programs often running silos which make them ineffective and lead to:

- Lack of visibility into risks
- Inability to address third party risks
- High costs

Developing these activities into a silo increases the likelihood that counterproductive objectives are established using suboptimal strategies.

This means that performance is not optimized for the greatest outcome and efficiency.

Integrating GRC capabilities within your organization does not mean creating a massive Department dedicated to GRC and getting decentralized management.

It does not call for using only a single GRC software system to manage it all. Instead, GRC is about establishing an approach that gets the right people the right information at the right times.

It works to establish the correct objectives, actions, and controls to address uncertainty.

Organizations that invest in GRC initiatives properly by integrating them across all of the organization see a number of benefits such as:

- Reduced impact on operations
- Improved information quality
- Reduced costs
- Reduced duplication of activities
- Improved ability to gather information efficiently
- Improved ability to repeat processes consistently

Investing in GRC benefits your entire organization through streamlining business processes and making compliance management easier.

With better corporate compliance, you can spend less time working about the risks of non-compliance, and more time focused on the areas of business that generate revenue to grow your company faster.

PLANERGY provides the flexibility you need to manage compliance activities when working with partners on regional or international level.

It has everything you need to automate procurement processes that are compliant with internal policies as well as regulatory requirements in your industry.

What’s your goal today?

1. Use PLANERGY to manage purchasing and accounts payable

We’ve helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our “Solutions” page to see the areas of your business we can help improve to see if we’re a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide “Preparing Your AP Department For The Future”

Download a free copy of our guide to future proofing your accounts payable department. You’ll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts