White Paper

Demystifying GRC

Abstract

Executives globally are highly focused on initiatives around Governance, Risk and Compliance (GRC), to improve upon risk management and regulatory compliances. Over time GRC has been looked and interpreted differently in many organizations but at broader level it includes organizational practices around corporate governance, enterprise risk management and corporate compliance.

Today IT teams face many challenges like data breaches, complex enterprise architectures and dynamically changing regulatory compliances. They have to be vigilant not only about advancements in the cyber-threats but need to adopt to evolving industry standards as well. These factors along with increased focus on accountability have sparked the organizational interest and inclination towards pursuing a broad range of governance, risk and compliance initiatives.

In the current complicated environment the organizational practices on GRC are still evolving. These initiatives many a time are run in silos and mostly lack coordination amongst teams, which exposes organizational to greater risks. Enterprises need to look at new ways to integrate these initiatives for an effective GRC model.

What Does GRC Include?

At its root the initiatives around governance, risk and control includes addressing three main components.

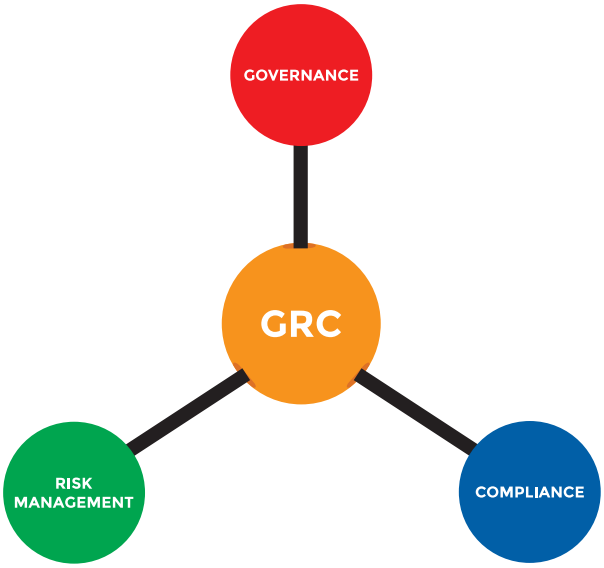
- Governance –

  It includes the management processes and approaches to ensure smooth functioning of the organization. These are critical to provide oversight and mitigation for business risks. The governance process varies across organizations but at a basic level it includes few common components like defining and communicating key policies, formulating control structures, specifying rights and responsibili ties among different stakeholders, setting up business scorecards for evaluating performance and most importantly it provides a framework to monitor and attain organizational objectives. Thus a strong governance process helps elevate employee and public confidence in the organization.

- Risk Management –

  Is a process which enables an organization to identify, analyze, evaluate and take necessary action on any perceived risk that might adversely affect the business. Organizations these days are extremely proactive in identifying and managing risks across a wide range of functions (e.g. operational, technological, financial/commercial, IT, regulatory, compliance) and executives are demanding dashboards to continuously assess the organization's risk score. Risk management has arguably become one of the key concerns for GRC model, helping organizations to methodologically identify, analyze, prioritize and respond to any risk. A response to risk could be in any of the four advocated ways i.e. Avoid, Control, Transfer or Accept.

- **Compliance –** Ensures that an organization has all the processes and controls in place to conform to requirements arising from various external and internal factors (i.e. government bodies, geo-specific laws, regulators, internal policies, contracts and industry standards). At organization level, achieving compliance is a complicated task and requires matured management processes capable of identifying applicable requirements, prioritize among them, take necessary actions to implement identified compliance controls and make compliance sustainable on an ongoing basis.



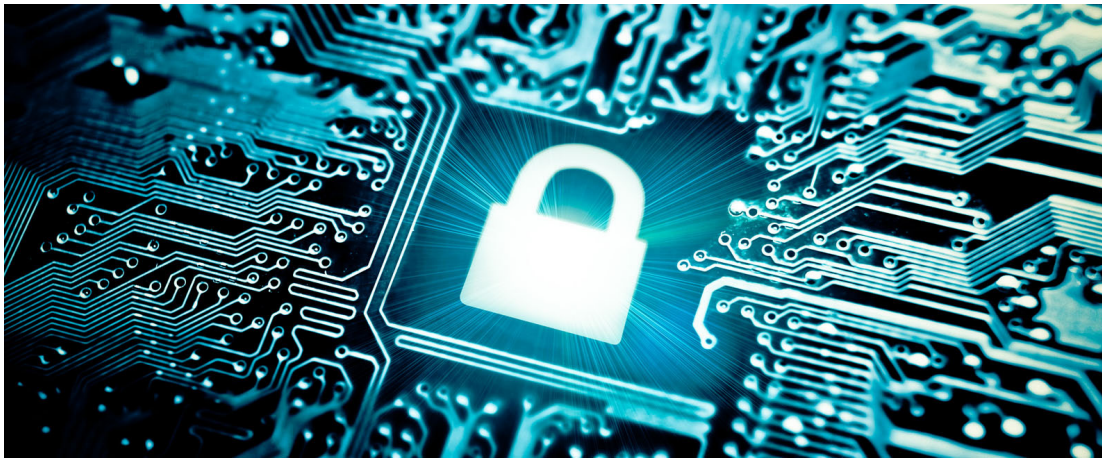
What Does GRC Include?

Each of the three elements of GRC (i.e. governance, risk assessment and compliance) is not a one-time activity. Growing regulatory requirements, evolving best-practices framework, new cyber-crimes and heterogeneous enterprise IT fabric has warranted that GRC processes need to be assessed time and again to ensure sufficient coverage at all times. Organizations have realized that GRC processes must be made into repeatable with higher flexibility to handle the agility of today's IT environments.

When organizations decide to implement GRC processes they are looking to invest heavily both in time and resources. More complex the underlying IT infrastructure, greater is the efforts and costs involved. Thus it makes all the more sense that these initiatives are structured in a way that the processes intrinsically become repeatable and allow any changes to be adopted at a faster rate and much reduced costs. GRC requirements can come from multiple unrelated sources and hence a unified, integrated and repeatable approach can save on redundant efforts, check on budget overruns and significantly reduce risks of non-compliances.

It is critical that a GRC solution should provide flexibility of tweaking and propagating the process changes through control, definition, enforcement, and monitoring so that an organization can leverage the solution to deploy a consistent framework across the organization.

Traditional Approaches and the Problem



Many Organizations are still following traditional approaches for managing GRC processes and struggling to get to operational efficiency and desired outcomes. Commonly used traditional approaches are described as below:

- **Manual Processes –** Policies are being managed using spreadsheets, PDFs or at most in a shared portal. These practices not only lead to redundant efforts across various divisions and systems but also make policy enforcement time consuming and inconsistent. This turns to be a perfect recipe for non compliances during audits as discrepancies become very obvious and intensified.

- **Separate Functions –** Most organizations still have different teams looking at each of GRC frameworks. These teams providing oversight are often from different departments or even from different locations. Such approaches can lead to disconnect and duplications between governance, risk and compliance functions. It also leads to significant gaps in the controls and make the solutions non uniform across organization.

- **Products working in Silos –** Due to lack of a holistic approach to GRC process, most organizations generally end up deploying multiple disjoint applications which run in silos to manage specific element. These systems pose financial and operational challenges as it becomes time consuming and resource intensive to implement any change which need be configured separately in each system.

What to look for in a GRC Solution?

GRC is still a relatively young discipline. This framework provides an alternate approach to traditional ways and provides a centralized approach to standardize polices and controls, ensuring a consistent rollout across the enterprise.It tries to leverage the commonalities between governance, risk and compliance elements, thereby enabling an integrated process to provide consistent approach to governance, risk and compliance functions.

Whilst there is no one set definition for a successful GRC solution, there are few key factors that can provide a benchmark to evaluate any solution. Common features from successful GRC implementation:

- **Support multiple controls –** One of the biggest pain points which led to silos of point solutions is lack of support for heterogeneous control points. A Successful GRC solution should be able to support large number of controls arising from government, operational and industry mandates.

- **Support multiple controls –** One of the biggest pain points which led to silos of point solutions is lack of support for heterogeneous control points. A Successful GRC solution should be able to support large number of controls arising from government, operational and industry mandates.

- **Policy lifecycle management –** Policy management is at heart of any GRC implementation. Organizations have fairly complex and time consuming procedures to handle various polices around employees, ethics, conduct, IT etc. It is critical that the GRC solution should provide an easy interface to not only define and implement various polices but to manage every stage of policy lifecycle with a single click.

- **Standardizing governance –** Solution should advocate standardized approach to implement corporate governance strategy encapsulating company's goals, performance measures and compliances.

- **Risk evaluation and treatment –** In today's challenging environment, it's impossible to have pre planned mitigation plan for all risks. Risks can potentially come from any channel be it internal or external. Therefore the GRC solution should provide a framework to reduce damage by identifying, analyzing and prioritizing risks such that high severity and probability risks are handled first. The solution should help with risk assessment and allow timely implementation of high-priority controls.

- **Agility towards change –** IT landscapes and continuously changing and so are the surrounding environments. A GRC solution therefore should have agile approach towards adapting changes. It should be easy to adjust and improve basis newer controls being introduced.

- **Auditing, Reporting and Analytics –** Integral to any systems effectiveness is its flexibility to monitor and report on the key controls and aspects. Successful GRC solutions have been able to provided top level management dashboards with flexibility of drilling down to granular levels. This helps organizations to keep track of their progress towards defined goals and targets. In addition it has a robust auditing mechanism to ensure full compliance.

About ARCON

ARCON is a leading Information Security solutions company specializing in Privileged Identity Management and Continuous Risk Assessment solutions. With its roots strongly entrenched in identifying business risks across industries, it is in a unique position to comprehend and identify inherent security gaps in an organizations infrastructure framework and build and deploy innovative solutions/products to significantly mitigate potential risks.