Governance, Risk & Compliance:

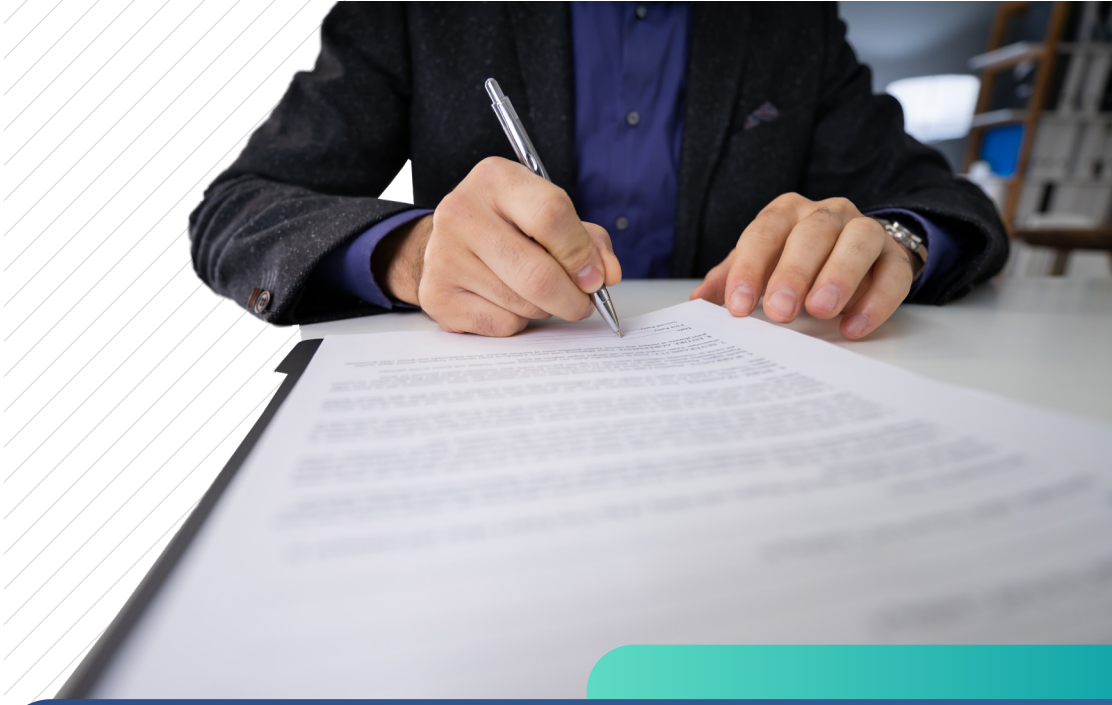
How Enterprises are Staying Safe in a Changing World

Managing Governance, Risk and Compliance (GRC) requirements is in many respects a losing battle for enterprises. Defending against “enemies” that constantly evolve, find new avenues for attack and can strike from anywhere is a highly disadvantaged situation for those charged with security in organizations, while the pressures of dozens of regulatory schemes across different regions are immense. As the pace of technological change increases, the ways in which organizations approach GRC will also need to evolve to meet the needs of security. In this eBook, we will look at how GRC is changing, and what to do with this information.

The Challenges facing GRC

Governance, Risk and Compliance is a difficult area to focus on for decision makers. Much like real-world security, if it is doing a good job, you won't notice it at all; only when security measures fail do you really see their importance. At least for enterprises, the issue is kept salient by the constant news stories of data breaches or regulations such as GDPR, though this only highlights how many enterprises have failed to maintain effective GRC functions. However, it is perhaps unsurprising that firms struggle; GRC is a complicated area that will likely have unique requirements for each business, demanding elegant solutions that are often beyond legacy GRC applications.

Of course, when discussing GRC challenges, we must mention the growing regulatory burden placed on companies around the world, particularly when it comes to data management. Enterprises have not helped themselves here, regularly abusing the trust placed in them by consumers and at the same time failing to properly protect private data from nefarious actors. This is an area that is difficult to predict as well, since it depends a lot on the vagaries of different governments; will a potential Biden government in the US follow the EU in demanding more control over data, for example?



Currently, the market for GRC applications is fragmented, with disparate teams addressing disparate issues through the firm, with little data synthesis. As technology and compliance requirements advance, this leaves enterprises exposed to greater levels of risk, and this is only exacerbated by greater demands for digital transformation. At the same time, enterprises have taken a "technology first" approach to solving risk and compliance issues, leading to a fragmented architecture that both fails to meet the needs of GRC and consumes large amounts of enterprise architecture resources.

The Key Competencies for effective GRC

Forrester Research believe there are 4 key competencies that determine whether an enterprise has a mature GRC function or not.

Oversight

Oversight relates to the holistic management of risk, and its alignment with the overall business strategy. GRC can involve many different functions of the firm, from Legal and HR to IT and Operations, which demands careful management.

Process

Process is the set of workflows used to manage risk and compliance, and maintain consistency. Strong standardized processes can support GRC issues across a variety of areas, even when they differ significantly.

People

People are the professionals who carry out the oversight and processes needed for GRC. Any successful GRC implementation will require talented people who are capable of building and maintaining the other competencies.

Technology

The Technology competency underpins the other 3, improving efficiency and decision-making ability – but immature technology can hinder the execution of GRC requirements.

Gartner

Integrated Risk Management is a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision making and performance through an integrated view of how well an organization manages its unique set of risks.

The Rise of Integrated Risk Management

If technology is a key competence for GRC, and legacy GRC technology is failing to keep up with the pace of change elsewhere, what can be done? Many organizations are now moving towards Integrated Risk Management (IRM).

The types of risk that may be included in IRM are:

- *Corporate Compliance Management – Increasing complexity of compliance with new regulations such as GDPR.*
- *IT Risk Management – The disruption of traditional risk models by IoT, machine learning and big data. New and emerging technologies will require a rethink on the sources of IT Risk.*
- *Business Continuity Management - The ability to identify, respond to, and recover from business disruptions is critical to the success of the modern digital organization.*
- *Third Party Risk – The reliance on complex vendor supply chains and geographical location issues.*

Overall, this is not particularly different from understandings of GRC, but Gartner stress that IRM solutions – technology providers focused on the broader, vertically aligned application of IRM, as opposed to the more focused GRC solutions – will address emerging challenges of GRC, while being better placed to grow with the organization and support future integration.

It is argued that to meet the challenges of risk, organizations need to be able to have a comprehensive view of all business functions and units, as well as key external relationships with business partners. This demands technology solutions that can take a much more collaborative approach, working across locations, business units and between business relationships. Forrester argue that any provider of GRC or IRM solutions should do the following:

- *Augment point-in-time risk assessment data with real-time monitoring*
- *Use AI to make risk management agile*
- *Provide advanced risk management capabilities*
- *Keep pace with regulations that will affect your business tomorrow*

Breaking down siloes between risk areas should improve decision-making and help to enhance business intelligence for the entire organization. The right IRM solution will make it possible to understand the wider business implications of risk management, and align GRC functions to strategic questions.

Despite the advantages discussed so far, GRC technology has a distinct first mover advantage. Convincing executives and other key stakeholders to shift towards an IRM approach is going to be an important part of evolving your enterprise's risk management. Educating stakeholders on the importance of organization level risk, as opposed to individual department risk, will go a long way towards convincing people of the benefits of IRM.

Summary

The shift toward an IRM approach means that GRC technology will have to evolve to better support scalability, risk aggregation and emerging risks, or die off and be replaced. It is likely that adoption of IRM will grow as organizations continue to increase their GRC maturity. Nonetheless, IRM technologies may not be the best choice for every organization. Forrester advise:

> *Consider whether the technology has been misconfigured or whether your GRC program's maturity has simply outpaced your GRC platform's capability*

Integrated Risk Management will not be necessary for every firm, due to the unique challenges that are posed in different situations. Forrester also highlight oversight as a key competency; being able to manage the entire risk function and its alignment with strategy. For enterprises that choose to move in a new direction for their GRC function, this can be a very important insight. Being able to maintain risk management and strategic alignment during transformation periods could be vital to preventing data breaches, hacks, or compliance failures. This is what Orbus offer through the iServer Suite, with the central repository model enabling risk analysis, traceability and mitigation regardless of the circumstances.

Rapidly Gain Visibility Around Compliance and Security Risks

Book a tailored demo today to find out how the iServer Suite can help you anticipate and prevent cyber-threats by identifying compliance and security risks

Book a Demo