TÜVRheinland®
Risktec

RISKworld / The Newsletter of Risktec Solutions / Spring 2022 p10-11

Governance, Risk and Compliance – A technology-led approach to managing risk

Most business leaders are hard-wired to seek growth opportunities and create value by taking risks. Risk management is often an afterthought and usually tackled by silos within the business. But organisations lose value by failing to manage risk routinely – it is crucial for the organisation to know continually what risks it is taking and that they are appropriately managed. Technology-based solutions for governance, risk and compliance (GRC) are being increasingly deployed to help achieve this goal.

WHAT IS GRC?

GRC aims to assure an organisation reliably achieves its business objectives, addresses uncertainty and acts with integrity.

- **Governance** is the corporate processes established and executed by the board of directors and reflected in the organisation's structure and approach to achieving goals
- **Risk** is about managing those threats to the organisation which could prevent it from reliably achieving its objectives (often called ERM - Enterprise Risk Management)
- **Compliance** refers to adhering with applicable laws and regulations, as well as the company's own policies and procedures

GRC aims to synchronise information and activity across these three facets in order to:

- Operate more efficiently
- More effectively share and report information
- Avoid wasteful overlaps

A BRIEF HISTORY OF GRC AND TECHNOLOGY SOLUTIONS

It is generally accepted that the structured approach to GRC arose from the Sarbanes–Oxley Act of 2002 ('SOX'), a United States federal law that mandates accounting practices for corporations. SOX was enacted in response to the major corporate and accounting scandals of the late 1990s and early 2000s, including Enron and WorldCom, which cost investors billions of dollars and shook confidence in public markets.

Unsurprisingly, given the complexities of managing different types of risks, the GRC efforts at large corporations in the early 2000s were siloed endeavours. There was the inevitable heavy use of spreadsheets and bespoke databases across functions such as IT, security, legal, finance, HR, HSE and customer service, for example.

By the mid-2000s a few specific GRC tools were coming on the market to help manage the processes and information, although most were focused primarily on IT controls. Today, there are multiple vendor platforms capable of managing the entire requirements of GRC. These digital tools overcome the technological challenges associated with operating global processes and thus remove any need to manage data in silos.

Some tools such as RSA Archer are specifically designed for GRC, whereas others like ServiceNow can do much more than just GRC and are able to automate the workflow for almost any business process.

STARTING THE GRC JOURNEY

When an organisation embarks on its journey towards successful risk management with a GRC programme, it needs to take a structured approach to aligning the GRC global platform with its IT and business objectives. Whilst the initial phase involves the introduction of a set of GRC tools and technologies, enterprises often fail to think through the entire technology implementation and forge ahead without sufficient analysis and planning.

An important first step is a meticulous process analysis to:

- Clearly define the project's objectives and capture the requirements and expected results
- Assess and understand the organisation's data
- Simplify and improve the GRC processes
- Propose a seamless GRC ecosystem of digital tools and technologies

The outcome of this analysis sets the stage for the subsequent design, build, prototyping, implementation, roll-out, training and performance monitoring phases, allowing GRC tools to evolve as the requirements or situations demand.

CONSIDERATIONS ALONG THE WAY

Some GRC projects can stall at the first step, as the organisation struggles to understand its data or gets bogged down in the complexities of its own GRC processes. This is where a technology-based solution can really help. Leading platforms have in-built GRC best practice processes and procedures, all of which can be readily customised. In this way, the technology becomes an enabler, helping the organisation to implement GRC processes more quickly and easily. Improvements can always be made later, following annual performance reviews for example.

Another important aspect of the GRC project is to focus on configuration rather than development. Leading low/no code tools are incredibly customisable and so it makes sense to use this functionality and flexibly adapt processes around the tool rather than unnecessarily over-engineer the tool. Instead of exhibiting a developer mindset – *"I need to re-code the tool to work the precise way I want it to work"* – the project is often better served by reducing complexity and standardising existing processes, with a view to future proofing to meet changing objectives.

The project team must be actively engaged throughout the entire implementation, to deepen stakeholder understanding of the project's objectives and the expected results. An educational approach needs to be taken to ensure users become acquainted and confident with using the tools.

Finally, a key consideration throughout the platform implementation is to address cyber-security threats. This requires a robust approach to risk management, including vulnerability and penetration testing.

CONCLUSION

Organisations reach a size where coordinated control over GRC activities is required to operate effectively. If tackled in a traditional siloed approach, the outcome will be duplicated GRC activities which increase operational costs, or incomplete GRC leading to unknown risk exposures.

In contrast, a GRC technology solution helps organisations to operate more efficiently, communicate more quickly and readily share information. When implementing a technology platform, the opportunity should be taken to create robust, standardised GRC processes to help future proof the solution.

Contact: Dev O'Nion
enquiries@risktec.tuv.com