IGNYTE ASSURANCE PLATFORM™

INTEGRATED GOVERNANCE, RISK, & COMPLIANCE BUYERS' GUIDE

Discover a Simplified Solution for a Complex Environment

Table of Contents

Integrated Governance, Risk, & Compliance Buyers' Guide

About This Guide

The purpose of this guide is to introduce you to the concept of integrated cybersecurity Governance, Risk, and Compliance Management and to provide practical considerations when purchasing a GRC platform. The guide is designed to provide a comprehensive view into the potential problems that that can occur if the wrong technology is selected. The information in this guide can be used to gain general knowledge about cyber Governance, Risk, and Compliance and aid in the evaluation of such products. Additionally, this guide can be used for creating a request for information (RFI) or request for proposal (RFP).

Current State of Cybersecurity Governance, Risk, & Compliance

The concept of GRC software was introduced over a decade ago with the onset of Sarbanes-Oxley (SOX) Act of 2002 and it became the primary driver for implementing automated GRC platforms across different industries. SOX is also known as the Corporate Responsibility Act that mandated strict reforms to significantly improve financial disclosures from businesses and prevent financial fraud. This was the beginning of a new era for first iteration of GRC software. Since then, SOX-built GRC platforms are continuously being modified to fit a wide variety of risk and compliance activities. Today, most GRC platforms have adopted a singular content framework that is known as "Unified Compliance Framework" (UCF). UCF serves as the primary IT content retrofitted into the original SOX-built GRC platforms. UCF is used to solve for all things IT GRC including IT Security Risk and Compliance.

> *"Legacy vendors are getting complacent with their technology road map and not keeping up with the more advanced product features and design that customers are seeing in other business applications,"*
>
> *- The Forrester Wave™: Governance, Risk, and Compliance Platforms*

As technology and businesses start to rapidly evolve, the legacy-approach to GRC platform development and content management is no longer effective. However, most Chief Information Security Officers (CISOs) are forced to continue to use their legacy GRC platform due to their company's initial investment. Regulators and various standards developing organizations prefer one standard over another to manage cyber risk and legacy GRC platforms, and, CISOs are aggressively seeking solutions that link GRC to support solving evolving cyber threats. Existing solutions are not built to handle multiple the types of emerging standards that dictate rapid change in existing business processes in order to address to address new threats.

"It is often said that GRC tools frequently fail due to lack of formal business processes; however, with the current state of rapidly evolving cyber threats, most tools lack the ability to quickly adapt to continuous evolution of business processes without significant investment of time and cost," states Max Aulakh, CEO Ignyte Assurance Platform.

Executives today are demanding modern Risk Management approaches that quickly adopt to emerging business processes, frameworks, and threats. Clearly, the GRC market is lacking true innovation.

"Legacy vendors are getting complacent with their technology road map and not keeping up with the more advanced product features and design that customers are seeing in other business applications," The Forrester Wave™: Governance, Risk, and Compliance Platforms

The following are key issues around the current state of cybersecurity governance, risk, and compliance systems:

- Executives & security executives prefer modern tools over legacy systems and legacy approaches
- Legacy systems have usability issues and lack innovation
- Legacy systems' development approaches require tremendous upfront customization and have significant development costs

Common Myths Surrounding GRC

Though, GRC is gaining wide adoption in the enterprise, covering areas such as operation and enterprise risk management, and incident management, among others, GRC utilization continues to be affected by a series of myths including:

MYTH #1

The best and most innovative solution must be on the Magic Quadrant or Forrester Wave

MYTH #2

The best solution must solve every single GRC use case in a single platform

MYTH #3

GRC implementation is too complicated, costly, and time-consuming

MYTH #4

GRC is a concept that organizations are compelled to implement by the government without other benefits to the firm

In truth, all businesses should recognize that organizational GRC activities help sustain operations, manage risks, and achieve compliance, which are all necessary for good governance. This concept is critical for organizations of any size. A GRC platform is vital for any organization that wants to align their cyber security activities to business goals while managing risks effectively and meeting all compliance requirements.

What Your Vendors May Not Tell You

In most cases, a GRC vendor will have a financial and emotional stake in their product, and organizations should understand their motivations before engaging in an expensive and stressful undertaking. Some vendors will share all crucial details with a client while a majority will not. Raez et al, (2011) note that while software vendors share a common basis in their GRC understanding, they deliver diverse functionality. At the same time, the product's technology architectures may differ in their degree

of integration. In all cases, the GRC vendor will present information that is more positive about them or their product. A candid conversation within any closed executive security community quickly reveals that most GRC projects are costly and often fail. Fortunately, this guideline highlights some of the most common reasons why those implementations didn't succeed.

Usability & Modernization Issues

Most GRC software solutions are built by developers and GRC professionals without consideration for usability in mind and require significant adoption through enforcement. This is one of the chief complaints of almost all current enterprise GRC software on the market and in the community in general. A quick google search on the terms "GRC software" will reveal the most existing GRC platforms interfaces have significant usability issues and resemble a user experience built from 10 years ago.

Hyper-Focus on a Single Solution to Solve All Problems

This issue is often cloaked as "Single Pane of Glass" or "Single Source of Truth." In most cases, it is often a fallacy to think that all GRC business problems and processes can be solved through a single technology. Most modern enterprises are breaking down silos by using advanced programming paradigms, such as micro-services versus using a single technology platform. GRC vendors most often attempt to solve all compliance and risk processes using a singular approach that doesn't align with business requirements or the actual regulatory requirements. Even one of the top security Gartner Analyst, Dr Anton Chuvakin, seems to agree with Chad Loder on his comment about "single-pane-of-glass" and forgetting the "people" part of GRC, while Archer and similar platforms seems to be rated near the top by Gartner Magic Quadrant each year.

Unclear Vendor Business Models

In many cases, external services firms, value added resellers, and partners are often incentivized to stretch the scope and costs of delivering a platform through unnecessary configurations, customization, and third-party engagements and deliberately push customers to purchase more than they need. It is imperative for businesses to know their vendor's business model.

Complexity of the GRC Software

Flexibility of GRC software can often mean complexity in configurations, leading to longer implementation times that require additional training and more customization than originally was planned. At the same time, the software may not live up to the business's expectations. In fact, many GRC platforms may end up creating extra work and require the hiring of additional developers while still not meeting critical requirements.

GRC Software Implementation

Vendors must sell their GRC certifications, training, and curriculum which are required to use even the basic features of the software. These contribute to long implementation cycles.

Lack of Sufficient Support

In some cases, the GRC software will break down entirely. Unfortunately, business will face difficulties while fixing it. This proves to be even more challenging when vendors don't provide the right level of support.

If an organization intends to invest in a pricey, sophisticated GRC platform, it is vital to consider the above factors to avoid selecting a software that gives insufficient output and lacks sufficient vendor support. This guide provides a proven approach for businesses to rely on for successful GRC platform selection and implementation.

Tips for Procuring a GRC Platform

#ThinkBeyond the Magic Quadrant

Industry Analysts Don't Actually Use the Product's They Rate.

Don't rely 100% on analyst reviews if you want GRC project success — analysts are useful in helping you understand basic issues around a specific GRC market. However, they should not be the primary consideration for your decision making. For the GRC vendors themselves, the industry analyst relationship falls under corporate communications and marketing activity. Therefore, analyst presentations, briefings, and criteria development are generally under sales and marketing department to help mold the analyst opinion. Businesses can use an analyst's opinion to get initial product details. However, it is important

for businesses to think beyond analysts' recommendations and make their own informed opinion about purchasing and deploying a GRC platform that will benefit the organization. Here is an excellent article by Ben Rothke, who serves as an advisor to CISOs on understanding Gartner and its limitations. This is a must read for any security team attempting to purchase security solutions.

Don't Boil the Ocean
Prioritize Your GRC Efforts

GRC covers a lot of ground — operational risk, compliance, cybersecurity, third party management, auditing, and so on — and incorporates hundreds of rules and regulations, dozens of policies, and scores of risk management activities. The activities seem complex and time consuming. However, while considering purchasing a GRC platform, it is important to address one activity at a time. Attempting to deploy an integrated solution for all activities at the same time would be too overwhelming.

Notably, prioritization in the GRC program can be deployed based on the nature of a business to establish important activities for an efficient GRC. Businesses can initiate a phased rollout of modules instead of running them all at once. The process can be started with a few crucial activities, and additional ones can be added gradually.

Select Specialized GRC Software with integration options
Versus A GRC Platform that Claim to Solve All Problems

No single solution or company has access to all the intricacies of specialties within GRC, yet many advertise their platform addresses all GRC problems. Ask your vendor which specific-use cases they have solved. Most GRC platform providers understand workflow management but lack the domain expertise mandated by certain information security risk management standards such as FISMA or FEDRAMP. These standards will not only shape your business processes but will determine if your new automation platform will meet specific requirements and organizational compliance objectives. Selecting a non-specialized tool increases the probability of failure and the likelihood of increased costs for consulting fees to make a workable solution. Additionally, the actual product rollout could be up to one or two years delayed, depending on the new software development schedule needed.

Get Started Now!

Give us a call to setup a demo today at https://ignyteplatform.com/request-a-demo/

REQUEST A DEMO

FOR MORE INFORMATION

To learn more about how Ignyte can help solve your business and IT challenges, contact your local representative or authorized reseller — or visit us at ignyteplatform.com. If you are an existing Ignyte Platform customer and have questions or require additional information about licensing, please contact Ignyte at support@ignyteplatform.com or call 1.833.IGNYTE1, (937) 789-4216.