windward

WINDWARD SOLUTION OFFERING

Governance, Risk, and Compliance

Overview

Companies must establish robust GRC platforms to mitigate the increasing risk of cybercriminals and evolving regulatory demands.

In today's complex business environment, enterprises grapple with regulatory compliance, cybersecurity threats, and operational risks. Navigating this evolving landscape requires a robust Governance, Risk, and Compliance (GRC) framework that manages these challenges while effectively driving business performance and innovation. However, traditional approaches to GRC often fall short of meeting the dynamic needs of modern enterprises. As organizations face increasing volume and complexity of regulations, the need for a comprehensive and agile GRC platform has never been more pressing.

windward

Most organizations struggle with GRC.

Market analysis has shed light on the issues organizations face when considering modernizing, optimizing, and accelerating their existing GRC program. While businesses are growing and increasing technology investment for mission-critical processes, **65% of organizations don't have an integrated, automated approach to managing IT risk**[1]. So, why are these organizations challenged? We investigated the challenges of implementing a new GRC platform.

The top concerns we've observed include:

- Reporting and performance metrics
- A lack of centralized data and platform
- Management of complex regulations
- Resource constraints, and
- Cultural resistance to change.

GRC involves managing multiple processes, regulations, and stakeholders, so an optimal solution must break down silos with a unified approach to delivering effective governance and risk management.

Creating a clear picture of GRC program status is crucial to conveying performance to leadership. This is difficult to accomplish when the program is fragmented and teams strain to produce accurate analytical representations. Disparate data sources are another key issue, making it difficult to gather the necessary data and track progress across departments. Evolving regulatory requirements also make GRC administration difficult, as end-to-end policy lifecycle management can be a resource-intensive process without specialized software solutions. These workflows contribute to overall resource constraints, as maintaining a robust GRC program requires significant resources, including time, budget, and skilled personnel. Finally, Cultural resistance to change is another challenge to implementing a new GRC program, as GRC professionals are long accustomed to conducting business through their current practices.

Successful deployment and support for GRC technology are foundational elements of a company's IT strategy.

Every organization needs a compliance framework tailored to its lines of business. However, how this is executed varies, with some organizations conducting GRC via spreadsheets and others utilizing cloud-based software. Leveraging technology and automation in a GRC platform offers significant value to all organizational stakeholders and reinforces consumer trust. Adherence to federal regulations directly impacts an organization's business continuity and financial standing, making GRC platforms a foundational element of its IT strategy.

GRC is a proactive approach to governance and risk management and implementing a modern platform provides various benefits that span across the entirety of an organization.

Firstly, a centralized framework for managing policies, procedures, and regulations provides **enhanced Governance capabilities**. By consolidating all policies and associated monitoring data in a central location, new functionalities are unlocked such as a unified approach to tracking and reporting, predictive and root cause analysis, and simplified audit procedures.

Leadership also gains high **visibility into GRC data with real-time** dashboards and reports. This is crucial for decision-makers, as the data is digestible, and areas of concern can be pinpointed with confidence. This data can also be translated into monetary savings from avoiding policy infractions or system downtime and the overall business impact of non-compliance.

Next, an effective GRC platform **streamlines compliance efforts** by automating data collection, audits, control monitoring, and reporting tasks. This increased program efficiency enables the various procedures for different policies to be executed with ease, giving resources ample time to address remediations. With the recent increase in the number of employees dedicated to risk and compliance[1] , process automation will deliver direct savings on payroll expenses and alleviate responsibilities attributed to complex policy management.

When organizations have separate compliance and risk teams, there are often **overlapping responsibilities** around developing policies and procedures to maneuver challenges. **48% of risk teams identified switching between risk management platforms as the most time-consuming task in their environment**[1]. While new tools are being introduced, the time it takes to complete responsibilities still increases, indicating a desire to shift from the typical tool sprawl to a consolidated platform that brings value to all teams.

Furthermore, a GRC platform **facilitates risk management** by integrating new tools like AI for risk analysis and monitoring. Organizations can thus implement proactive risk management strategies that identify issues before they arise, reducing the likelihood of negative business impact.

Finally, a GRC **platform fosters collaboration and communication** across different departments involved in GRC activities. This promotes a culture of transparency and accountability within the organization while breaking down long-standing silos.

Overall, the value of implementing a GRC platform lies in its ability to enhance governance, mitigate risks, streamline compliance efforts, improve decision-making, and foster collaboration. By investing in a GRC platform, organizations can effectively manage their regulatory obligations, protect their reputation, and drive sustainable business growth.

Effective implementation depends on detailed planning and a tailored approach to meet an organization's needs.

Windward's approach to deploying a successful Governance, Risk, and Compliance platform is centered around careful planning and execution. We have identified three stages in an organization's GRC platform journey to guide our methodology: Modernize, Optimize, and Accelerate. Although every organization has an established GRC program, the utilization of technology to drive efficiency varies widely. **Only 58% of organizations are confident with their ability to address compliance concerns**[2], indicating the ever-present need to innovate.

Our methodology is predicated on finding flow. The delivery of GRC program services is broken down into five key phases, designed to assess the current state of an organization's Governance, Risk, and Compliance framework and deliver high-impact technology that streamlines processes and reporting while maximizing observability.

1. **Assessment and Planning: (Modernize)**

Conduct a comprehensive assessment of your organization's GRC needs, including critical stakeholders, pertinent regulatory requirements, existing processes, and potential risks. Then, outline critical objectives and success criteria in a detailed deployment plan. This will provide an understanding of the current state and clearly articulate the delivery timeline's coverage.

2. **Vendor Selection and Customization (Modernize)**

Evaluate GRC platform vendors based on your organization's specific requirements and select a platform that addresses your needs. Customize the platform to fit your organization's processes, workflows, and policy requirements. This stage is where we make the platform yours—we design it to function optimally for your specific organization.

3. **Pilot Testing and Training (Optimize):**

Conduct a pilot test of the GRC platform in a limited environment where we identify any bugs, gather feedback, and make necessary adjustments. Provide comprehensive training to help you use the GRC platform effectively, including best practices and guidance on the various functionalities. This testing phase of the platform allows users to get familiar with the new software and address any performance concerns before pushing it to production.

4. **Deployment and Integration (Optimize):**

The GRC platform will be deployed in stages, starting with core functionalities and gradually expanding to additional modules and departments. We will ensure seamless integration with existing systems, including ERP systems, risk management tools, monitoring software, and document management systems. Users will begin using the new platform to conduct business, and deployment will be closely monitored to promptly address any technical issue or user concern with minimal disruption.

5. **Continuous Improvement and Evaluation (Accelerate):**

Establish processes for ongoing monitoring, evaluation, and improvement of the GRC platform. Stay informed about regulatory changes and evolving risk factors impacting your organization and update the platform according to regular system performance assessments. This stage fosters a culture of continuous learning and improvement, encouraging users to share insights and suggestions for enhancing the GRC platform's effectiveness.

By following these steps, organizations can successfully deploy a GRC platform, enabling better governance, risk management, and compliance across the enterprise.

GRC is not just a CISO issue; everyone has to be involved.

Typically, several vital stakeholders recommend or buy a Governance, Risk, and Compliance (GRC) solution. An investment in a new GRC platform would require input and signoff from various teams, which we have segmented according to the primary buyer for a solution and the stakeholders impacted by any decision.

Primary buyers in the organization dictate budgetary spending regarding a GRC solution and are responsible for program performance. Chief Risk Officers, Chief Information Security Officers, Chief Compliance Officers, and Risk and Compliance managers are heavily involved in GRC programs with the authority to reimagine the delivery of program components.

Additional stakeholders such as CEOs, CTOs, COOs, internal audit teams, and procurement teams are also called upon to provide input on current program performance, the organization's resource constraints, or expert advice regarding the regulatory landscape.

Effective collaboration and alignment among these key stakeholders are essential for successfully recommending and buying a GRC solution that meets the organization's needs and objectives.

Sources:

1. 2024 IT Risk and Compliance Benchmark Report, HyperProof.io
2. 2023 Risk and Compliance Report, Thomson Reuters Institute
3. The Forrester Wave: Governance, Risk, and Compliance Platforms Q4 2023, Cody Scott, 12/5/2023.