WHITE PAPER

CIO Strategies for Aligning GRC with Business Priorities

Sponsored by: EMC Corp.

Vivian Tero
Christian A. Christiansen
Cushing Anderson

July 2012

IN THIS WHITE PAPER

Today's businesses operate in complex, geographically distributed, and highly dynamic environments. The confluence of legal, regulatory, technology, and business developments increases the complexity and scope of an organization's existing GRC program. Because of the pervasive role technology plays in business and risk, CIOs are in a unique position to be a driving force to facilitate a more proactive alignment between the operational requirements of the business and the rapidly changing governance and compliance framework. This IDC white paper illustrates how several CIOs have employed practical, effective strategies to:

- Gain organizational buy-in to improved GRC protocols.
- Establish and maintain momentum for change to ensure long-term success.
- Demonstrate the value of a sound information governance program to support business imperatives.
- Embed risk and compliance awareness into business operations and ensure compliance.
- Leverage existing investments in dashboards and other monitoring technologies to efficiently transition to a stronger control environment.
- Avoid change overload through a phased, inclusive process.

SITUATION OVERVIEW

CIOs see several dynamics converging to make their role more central to managing risk:

- An uncertain legal and regulatory environment
- The explosion of digital content
- The migration of consumer technologies into the corporate setting

These dynamics represent a challenge for the enterprise but an opportunity for CIOs to build a more complete and meaningful risk management program. The sections that follow illustrate the strategies several CIOs used to help their organizations adapt to these complexities while increasing their business flexibility and better controlling their corporate risk profile.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

Complex Legal and Regulatory Landscape

Rapidly changing regulatory environments is one factor that exacerbates the complexity and scope of existing GRC programs. Most typical IT and organizational risk management programs isolate specific compliance requirements as independent GRC disciplines (security, compliance, enterprise risk, IT risk, corporate compliance, and governance, etc.). As a result, governance across these silos of compliance and risk management becomes weak, reactive, and static.

To compound that situation, an organization's risk and compliance profile is frequently dynamic. Changes in the legal and regulatory landscape require regular reassessment and updates to comply with new requirements. Scattered and disjointed silos limit visibility of the true nature of the organization's risk and compliance posture.

Proposed Regulation: Data Security and Breach Notification Act of 2012

For example, in June 2012, several U.S. senators proposed the Data Security and Breach Notification Act of 2012 (S. 3333) to compel covered entities to disclose corporate loss of personal customer data. Failure to provide a timely disclosure to the affected consumers and various federal agencies could result in fines of up to a half a million dollars. This bill is the fourth attempt to create a national standard and would supersede existing laws in all 50 states.[1]

The complexity of this law can illustrate some common challenges of the rapidly changing compliance landscape: As a first step, the regulation requires covered entities to assess whether a breach has caused or will likely cause identity theft or other financial harm. That assessment can trigger several reporting thresholds and notification requirements based on the nature of the personal data and on the likely cost of notification. This may either clarify or obfuscate a regulatory environment where 38% of Fortune 500 companies made a "significant oversight" by not mentioning privacy or data security exposures in their public filings, according to one survey.[2]

It is not just proposed regulations that cause potential problems. Reconciling and streamlining older regulations with new cloud-based businesses is also challenging.

Customer Example: Cloud Service Provider

Consider, for example, a publicly listed information management cloud service provider (CSP) with international operations. The CSP is obligated to comply with the Sarbanes-Oxley Act of 2002 (SSAE 16) audit standards as well as with the data retention, information security, and privacy regulations across multiple national jurisdictions. As a custodian of its customers' business and legal information, the CSP has to meet the compliance, security, availability, resiliency, and data integrity requirements for each of its 300,000+ customer accounts. Prior to the adoption of an enterprise-wide GRC program, the CSP was challenged to ensure individual customer service contracts were compliant with its broader corporate governance guidelines. Incident management, response and remediation, and customer compliance audits were inefficient and fraught with inconsistencies.

The CIO's team worked closely with corporate governance and the business unit leaders to redesign and overhaul the CSP's enterprise GRC strategy. To improve organizational focus on the changing protocols, the CSP staggered the rollout of its enterprise GRC program in a two-step process:

- First, the CSP established a comprehensive information process by adopting common standards and automating processes for policy management, compliance life-cycle management, and audit management.
- Second, the CSP leveraged previous compliance and risk management technology investments to improve security and incident management, risk assessment, business continuity, and vulnerability management procedures.

This two-step process illustrates a practical solution to avoid change overload while initially gaining organizational buy-in and momentum for change and then leveraging prior investments in supporting technologies.

Massive Growth in Retained Data

In an information society, information is money. Between 2005 and 2011, enterprises spent $4 trillion on the hardware, software, services, and staff to create, manage, store, and ultimately derive value from the massive and expanding digital universe. The importance of information to the success of enterprises results in another factor driving the CIO role closer to the management of risk: growth in retained data.

IDC's Digital Universe Study estimated the amount of digital information in storage surpassed 1.8ZB (1ZB or zettabyte = 1 trillion gigabytes) in 2011 and predicts retained data will double every two years. More importantly, at least one-third of the total digital universe must be assessed and managed for compliance, legal, and security requirements. And, of course, businesses increasingly need relevant and accurate information delivered to the right decision makers in a timely fashion to facilitate deeper customer insight and to identify and exploit market opportunities or operational efficiencies.

With the demand for information growing, it is clear that enterprises will capture, retain, and leverage ever increasing volumes and types of data. This massive growth of retained data presents IT infrastructure challenges in management, governance, stewardship, risk management, compliance, security, and data quality. While these disciplines have typically operated as discrete functions within an organization, the demand for more timely and reliable information requires ever more effective information governance.

Customer Example: Pharmaceutical Company

An international pharmaceutical company planned to leverage cloud services and big data technologies to support data management and analysis requirements for its cancer research activities. It determined that secure information sharing of patient research data across its research and business units was critical during drug discovery and clinical trials. However, it needed to reconcile the operational benefits of sharing data and compute resources against global data privacy and cross-border data transfer

mandates, as well as data sharing restrictions across the various research units. Achieving this balance required highly granular data segregation protocols and normalization of the relevant data classification schemas and information management policies. Adding to the complexity, the pharmaceutical company was simultaneously updating its privacy program to align with changes to the EU Data Protection Directive.

To balance these multiple objectives, the organization adopted an enterprise-wide privacy program with information governance as the cornerstone of the initiative. Key protocols and standards for privacy were incorporated in its cloud migration and big data implementation strategy. Additionally, critical GRC milestones were developed that included the identification of data stewards and the articulation of shared responsibilities and accountabilities across the business, research, and IT domains.

This implementation of a comprehensive program illustrates this organization's awareness that the value of a sound information governance program extends beyond simple compliance — effective information governance can effectively support a business imperative.

Migration of Consumer Technologies into the Corporate Setting

While emerging technologies, including cloud or big data leveraged by the pharmaceutical company profiled, can offer critical business benefits and market opportunities, new technologies also disrupt traditional operating paradigms. The deployment of new technologies into an already porous IT network introduces new risk management and compliance challenges. CIOs are becoming increasingly responsible for leveraging new technologies while effectively identifying and addressing threats that impact the organization's risk and compliance posture. The most relevant near-term IT drivers of new technologies must include rapid penetration of consumer-oriented devices deployed in corporate environments, as illustrated by "bring your own device" (BYOD) strategies in many enterprises. But other technologies, such as intelligent connected devices, automation, and machine-to-machine communications and transaction, are also introducing unfamiliar risk vectors to the enterprise.

As a result of these technology developments, CIOs are more often partnering with the C-suite to incorporate IT risk and compliance awareness into the operations and governance culture of the organization. Enterprise practices on the acquisition, provisioning, and use of business services and technology devices must effectively balance enterprise business objectives with risk and compliance obligations. When risk and compliance awareness become baked into employee communication, training, and incentives, the enterprise can better leverage new technologies, confident that new exposures are well understood and mitigated by appropriate controls.

Customer Example: Technology Manufacturer

A global high-tech manufacturing firm wanted to embrace the convergence of emerging technologies and smart devices. Corporate leadership believed that, if deployed judiciously and controlled with appropriate policies, new technologies could improve productivity and enhance the firm's competitiveness while increasing security

and improving information control. To achieve the balance between deployment and control, the organization engaged employees from the beginning. The company formally engaged its employees to review evolving policies and processes related to the acquisition, provisioning, and acceptable use of these technologies. At the same time, global data governance standards were also updated with employee involvement.

In parallel, the organization updated its risk management model to incorporate more contextual and situational awareness. Processes and some automation allowed the company to spot certain indicators of "risky" events or activities keyed to such information as employee role and authentication, device environment and location, and application and content environments.

This approach enabled risk and compliance awareness to be embedded into business operations. As a result of better visibility into risk activities, the company could adopt a multitier risk management model where enhanced security capabilities are based on those key attributes (role, location, device, application, and content).

HR was also deeply engaged in policy creation and change management. It had a key but indirect role in the enforcement of these policies: It ensured that governance standards compliance was integrated into individual performance and incentive programs. This ensured that everyone had skin in the game.

FUTURE OUTLOOK

The Evolving Role of the CIO in GRC

While a CIO's role supporting the technology infrastructure and ensuring business value for technology remains, the posture CIOs adopt to support an effective GRC strategy may be more important. As technology plays an ever increasing role in both the execution of business and the control of business operations, successful CIOs are at the nexus between business, IT, governance and compliance. To effectively manage this position, CIOs are increasingly called upon to develop a GRC strategy to align business, IT, and governance domains. CIOs are being asked to articulate the business risks and benefits of technology and how to better leverage technology to improve GRC compliance. In each of these areas, CIOs are engaging the C-suite, successfully supporting both operational success and effective governance and compliance.

Leverage GRC Strategy to Align the Business, IT, and GRC Domains

For successful enterprises today, CIOs are helping break down functional barriers between IT and corporate compliance, IT and enterprise risk management, IT and security operations, and IT and operational risk. In many enterprises, these functions have become disconnected as a result of acquisitions, reorganizations, or divergent operational priorities. And now, these disparate risk and compliance organizations struggle to scale up or collaborate in response to external developments.

IDC has identified two core priorities that CIOs commonly leverage to establish a cohesive enterprise GRC program:

- **Information and organizational governance.** With the support of the C-level suite, CIOs establish a common language for risk and compliance classification as well as define baseline thresholds, processes, and standards for measurement, monitoring, reporting, mitigation, and remediation of identified risks. Common business language, metrics, and standards are used to identify dependencies across various GRC, IT, and business domains.

- **Standardized and automated risk assessment processes.** CIOs have begun to establish activities and protocols to support ongoing improvements to the enterprise risk and compliance programs. These activities define accountabilities and shared responsibilities across stakeholders and business owners and establish standardized interactions.

A well-integrated GRC program hinges on cross-functional coordination, collaboration and shared responsibilities, and decision-making among key stakeholders, with the CIO providing leadership on all technology-related issues.

In the profiled pharmaceutical company, the data governance program normalized the various data classification schemas, identified and defined shared responsibilities and accountabilities of the data stewards, and developed common processes and standards for secure information sharing. The CIO's office leveraged security and data management classification schemas and ITSM service management standards to identify and map interdependencies across the various GRC disciplines. This was the critical step that enabled key stakeholders to recognize and define areas for shared objectives and responsibilities.

IDC believes there is no single approach for enabling the alignment of enterprise GRC programs. The path an organization takes depends on its technology and process maturity and on its existing GRC investments. While the profiled high-tech manufacturer executed an inclusive bottom-up approach, the profiled cloud service provider CIO worked with the corporate governance board to establish information flow and governance process and then improve specific high-priority procedures in a more top-down approach.

IDC finds that regardless of the approach, most successful organizations focus first on coalescing on the governance and stewardship issues and then on aligning processes to support the business objectives.

Leverage Business Value of GRC to Engage the Business

Because of the increasingly broad range of events that can trigger programmatic risk assessments, CIOs have had to shift from regulation- or control-centric value propositions to a more agile orientation that pragmatically integrates risk with the various business operations and IT domains. These events are as common and far reaching as:

- The introduction of new products or service delivery models

- Changes to existing partner ecosystems

- M&A activities
- IT replacement, restructuring, upgrade, or decommissioning cycles
- New regulatory and legal mandates

With each of these events, IDC observed successful CIOs at the forefront of identifying issues and offering both technical and process alternatives when events trigger programmatic risk assessments. These proactive solutions support the business value of GRC by increasing the stability and predictability of operations and helping ensure appropriate agility to activities within an understood and manageable risk profile.

By using processes and tools to demonstrate the dependencies across business operations, IT operations, and risk and compliance constraints, CIOs can effectively engage the business within the various GRC domains. This includes appropriate adoption of:

- Relevant portions of key standards (COSO, ITIL, ISO 270001, etc.) and the integration of these standards into an enterprise risk and control framework
- Programmatic risk assessments that take advantage of standards and best practices for the identification and business impact assessment of emerging technologies
- Standard processes for collaboration between legal and compliance functions to effectively assess and plan for emerging legal and regulatory mandates
- Formal, proactive communication of agendas, priorities, decisions, and responsibilities across relevant domains
- Structures and incentives to limit the number of decision-making layers

Each of these frameworks helps achieve the right balance between control and flexible processes by ensuring early awareness and timely, efficient communication.

The CIO of the profiled high-tech manufacturer leveraged existing protocols to engage business leaders while also involving information workers at every stage of the policy change. As a result of communication and agenda frameworks, the CIO worked seamlessly with the business owners to determine strategies for leveraging new technologies and also facilitated involvement of HR to ensure incentive alignment. Once the linkage between business strategy and performance incentives was clearly defined, employees were less likely to circumvent policies, and the standard communication protocols facilitated a smooth, predictable and, most importantly, compliant policy change.

Leverage Technology to Support Active, Efficient Governance

An array of both established and innovative automation, visualization, and analytics technologies can be effectively employed to ensure that business and GRC domains are able to access and view relevant, timely information. This insight enables leaders to make timely business decisions in the context of both the existing and the possible risk and compliance profile of the business.

Customer Example: Financial Services Organization

A global financial services organization wanted to improve the integration of its GRC program with its business decision making. To do this, the company worked with an external partner to assess its GRC maturity and define its GRC strategic road map. As a result of the assessment, the company:

- Implemented policy and governance standards that mapped to its top IT security standards
- Enhanced its capabilities to track and assess risk and compliance throughout the company
- Automated FFIEC compliance activities through a centralized management framework

The results of these changes provided management with better visibility into business decisions with risk integrated into meaningful executive dashboards.

The CIO, in collaboration with compliance, risk management, and financial risk and trading operations, helped ensure the resulting solution was adapted to existing compliance, risk identification, analysis, and remediation activities. The CIO also enabled the company to leverage its existing investments in dashboards and other tools.

EMC GRC Advisory Services

EMC GRC Advisory Services are designed to help organizations effectively adapt their GRC programming to the changing risk profile of their operations. EMC Consulting delivers this GRC-centric service offering to clients. EMC consultants support CIOs as they transition from siloed and reactive compliance and risk management initiatives into integrated enterprise GRC programs. EMC GRC Advisory Services can assist clients with:

- **GRC Program Strategy and Strategic Planning.** EMC Consulting works with the client to assess and define the scope of its GRC program as well as assess the maturity of existing discrete compliance and risk management programs.
- **GRC Program Development.** EMC Consulting works with the client to develop a program for understanding its risk profile, including defining the client's risk hierarchy, appetite, and risk ratings as well as developing the appropriate risk reporting framework, metrics, and risk remediation process and plan. EMC Consulting also assists clients in developing and implementing the appropriate GRC Program Governance Model.
- **GRC Program Management Optimization.** EMC Consulting and the client develop and execute an integrated and optimized GRC program. EMC Consulting develops use cases with the client and formulates detailed project process and implementation plans. To ensure successful adoption, detailed change management, communications, and training programs are also developed.

By leveraging EMC processes and technology expertise in advanced security, availability, data and process management, and infrastructure management, EMC Consulting's GRC Advisory Services enables its clients to:

- Define, develop, and manage a comprehensive GRC program based on specific business and regulatory requirements and stakeholder needs.
- Formulate and implement a solid GRC strategy and facilitate optimal GRC operations management for highly complex and dynamic technical environments.
- Transform discrete and reactive risk management and compliance efforts into an integrated GRC program to align processes and controls to support diverse business objectives, corporate policies, and industry standards.

Challenges

IDC has observed a few potential challenges that firms like EMC must overcome to help clients successfully create an integrated GRC program:

- **Organizational resistance to change.** Implementing an integrated GRC program often requires organizations to overhaul organizational, process, and technology philosophies. Organizational sponsors, and their consultants, must be able to overcome the natural resistance to changing processes.
- **Silo mentality.** Functional owners are inclined to operate in their own spheres. Successful programs IDC has observed develop and adopt standardized processes for measuring GRC maturity and success to help illustrate the ongoing value of an integrated GRC program to the enterprise. The process of continually reinforcing the benefits of a non-siloed program helps inculcate systems thinking and supports a more aligned organization.

CONCLUSION

Rapid changes in business, technology, and regulatory drivers make maintaining a disjointed and reactive compliance and risk management program unsustainable.

A comprehensive enterprise GRC program provides an integrated view of the risk and compliance posture as well as enhanced visibility and transparency to support decision making. To do that, CIOs have transitioned to more effective GRC programs by leveraging:

- GRC strategy to align the business, IT, and GRC domains
- Business value of GRC to engage the business
- Technology to support active, efficient governance

Despite the presence of organizational, financial, and technology hurdles, CIOs have employed practical strategies to help respond to and lead the drive for more integrated GRC programs. CIOs have been able to gain organizational buy-in to

increased GRC protocols and to ensure compliance by demonstrating the value of sound information governance in support of business imperatives.

While CIOs work to support these transitions, they should consider engaging providers that can demonstrate:

- Deep domain and process experience in enterprise risk and compliance management programs
- Experience in change management
- The ability to work across functional areas
- Technology and infrastructure expertise to handle complex and rapidly evolving IT environments

SOURCES

1. Senators Float National Data Breach Law, Take Four, *InformationWeek,* June 25, 2012, accessed June 29, 2012
2. Senators Demand Public Companies Disclose Data Breaches, *InformationWeek,* May 13, 2011, accessed June 29, 2012