WHITE PAPER

The Case for GRC: Addressing the Top 10 GRC Challenges

Sponsored by: EMC Corporation

Vivian Tero

December 2012

IN THIS WHITE PAPER

Businesses today operate in complex and highly dynamic global environments. Successful execution of business strategies requires an ability to effectively balance revenue generation and operational efficiency objectives with risk management and compliance obligations. This IDC White Paper discusses the top 10 governance, risk, and compliance (GRC) challenges that organizations are facing and the technology-enabled solutions they are employing to effectively execute GRC objectives. A typical enterprise encounters several of these challenges at any one time. It thus makes sense for enterprises embarking on or in the middle of a GRC journey to consider an integrated, holistic, and programmatic approach. This approach supports enterprise transparency on the critical dependencies and accountabilities across business operations and siloed GRC programs. It also allows for better leverage and optimization of enterprise assets and investments.

This document complements *CIO Strategies for Aligning GRC with Business Priorities,* an IDC white paper published in August 2012 that discusses the practical strategies CIOs used to gain organizational buy-in, establish governance programs that are aligned with business imperatives, and embed risk and compliance awareness into the fabric of the business.

SITUATION OVERVIEW

Why Governance, Risk, and Compliance?

In 2007, close to 90% of the organizations IDC surveyed had obligations to comply with at least three compliance programs. Five years later and despite efforts to adopt standards and automate processes, organizational and technical issues continue to stymie actions to address costs, eliminate compliance conflicts and gaps, and prioritize remediation activities. High-profile violations and data breaches are stark reminders that organizations remain susceptible even after passing recent audits, leading some to become dismissive and cynical about GRC. Compliance and security challenges are like the mythical Hydra; just when businesses think they have tackled a compliance or security challenge, another one appears to take its place. Businesses continue to grumble about the ongoing costs and risks associated with siloed compliance programs. In the meantime, new developments add to existing governance, risk, and compliance challenges:

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

- New regulations continue to come down the pipeline. For example, organizations continue to ramp up for the Dodd-Frank Act and the Affordable Healthcare Act. There are proposals to update the U.S. 1986 Electronic Communications and Privacy Act, as well as new bills to address cybersecurity and digital privacy. Overseas, the update to the EU Data Protection Directive is under consideration by the EU member nations.

- Business divestitures and new market, new product, and new business transformation activities continue to disrupt existing business models and trigger changes to the underlying IT infrastructure. Changes to business activities are typically accompanied by the deployment of emerging technologies. These developments, in turn, alter the existing information supply chain, create new data types and data models, and expand current IT infrastructure security perimeters. These developments underpin the aggressive growth in digital data.

- Big data is on the rise and demands an assessment of existing governance, risk, and compliance protocols. The digital universe surpassed 1.8 zettabytes in 2011 and is forecast to grow at more than 60% year over year, where 30% to 45% of total data must be assessed and managed for its security, risk, and compliance profile. Consider, for example, socially engineered attacks that take advantage of social networking to deliver a "malicious payload" into the target's device, control the compromised device remotely, and eventually gain entry into the corporate network and access valuable corporate information. Socially engineered attacks are not easily detected by traditional security tools until after a comprehensive forensic analysis, post-breach. Big data technologies can be used to pull information from various data sources and enhance situational awareness and detect and predict potential sources of fraudulent behavior before it happens. Also, the data types created are varied and, in many instances, in new content formats. For example, 74% of organizations already have a presence on the major social networking sites, while 46% already allow personally owned PCs as a primary work device. Many of these new data types are highly dynamic and transitory. The combination of big data attributes (volume, variety, velocity) challenges traditional tools and methods for extracting value. Their value comes from the ability to capture, discover, and analyze data from multiple sources and combine these to create new sets of valuable information and processes. The outcomes of these big data projects create new privacy, information governance, and regulatory obligations. Today, less than 20% of businesses have existing big data projects. However, anecdotal information on IDC end-user inquiries suggests a strong interest among businesses to accelerate these initiatives. The economics and infrastructure requirements of big data suggest that the majority of these solutions will be delivered and accessed by employees and customers through the cloud. By 2015, 20% of total information will pass through the cloud, and by 2014, 70% of organizations expect the majority of their employees to work outside corporate headquarters. Existing governance, risk, and compliance postures, policies, and controls must therefore be evaluated for the impact of changes to IT-enabled business activities.

Instead of becoming cynical or dismissive about the state of their GRC programs, effective businesses view the confluence of business, technology, legal, and regulatory developments as an opportunity to address the gaps and weaknesses in the programs. Effective GRC champions (such as CIOs, CROs, and CISOs/CSOs) are taking advantage of business transformation initiatives to address the failures that stem from disjointed execution, organizational apathy, and misalignment of stakeholder agendas. In parallel with efforts on organizational and process alignment, GRC champions also support initiatives to leverage process and technology for introducing efficiencies in risk management and compliance activities.

IDC interviewed several organizations about their enterprise GRC programs and their most pressing challenges. The key findings are discussed in the subsequent section.

Top 10 Risk and Compliance Challenges

1. **Management complexity of risk and compliance programs.** Management complexity stems from:

   - Lack of board-level oversight and program management of the organization's enterprise risk and compliance program
   - Absence of enterprisewide standards and protocols
   - Inability of the GRC platform to provide a transparent system of record and support collaboration for orchestrating key activities across business and GRC domains
   - Inability to identify policy, process, and control gaps and redundancies, leading to inefficiencies and conflicts in key risk and compliance activities

   The *Governance of Enterprise Security: CyLab 2012 Report* by Carnegie Mellon CyLab finds that corporate boards are still not undertaking key oversight activities related to IT risks and security. At the operational level, many organizations with multiple, siloed compliance and risk management programs are still using Microsoft Word, Microsoft Excel, Lotus Notes, and Microsoft Access to document policies, processes, and controls and to maintain the inventory of assets and resources associated with these controls. This results in duplication of effort, limited visibility of policy requirements exceptions, and lack of transparency on the critical dependencies. Process and cost inefficiencies abound in activities such as audit management, incident response, investigations, crisis management, and legal risk management. Lack of transparency impedes efforts to prioritize risk remediation and mitigation efforts. Organizations are slow to respond to incidents and potential failures.

2. **Organizational alignment of risk and compliance metrics and controls across functional domains.** Absent an organized and transparent "system of record" and collaborative process life-cycle management system, businesses are unable to develop and maintain a common language around data classification, process standards, and risk and compliance metrics. The inability to define common standards and metrics across the functional domains makes it difficult to expose the dependencies across these disciplines. When this happens, it

becomes difficult to solicit the relevant buy-in and define the shared responsibilities and accountabilities across business and GRC stakeholders. Critical stakeholders are unable to develop "skin in the game."

3. **Managing regulatory complexity to reduce the cost of compliance.** A typical enterprise with global operations has at least three global risk and compliance programs, in addition to regional/country-specific programs. Regulatory complexities stem from:

   - Administration burden associated with hundreds, if not thousands, of requirements and control objectives for each discrete compliance and risk management program
   - Inability to identify overlaps (such as common controls that could be shared across compliance mandates), gaps, and exemptions across risk and compliance (Business and system owners are also burdened by multiple assessments that ask the same question in different formats and the expense of maintaining duplicative controls.)
   - Inability to programmatically assess and identify potential changes to requirements, control objectives, and metrics when current regulations are amended or a new regulation is introduced
   - Inability to assess for risks and identify and change requirements when the organization deploys new technologies, launches a new product, and enters a new market (The introduction of a new regulation, new amendments to existing regulations, and deployment of new technologies add a new layer of complexity and cost overheads.)

   Standalone programs result in stakeholders missing out on the opportunity to develop common standards, pool resources, and reduce the overall burden on running the organization's risk and compliance programs. Business and system owners are also burdened by multiple assessments, adversely impacting employee productivity.

4. **Privacy and intellectual property protection.** The convergence of regulatory, legal, and technology trends increasingly taxes current capabilities to sustain privacy and intellectual property protection programs:

   - The data created is highly dynamic and based on emerging data models, thereby causing organizations to rethink their existing security, information governance, and privacy models.
   - Regulatory complexity challenges businesses to navigate a myriad of local-, state-, and country-level privacy and breach notification regimes. In the United States alone, there are over 20 federal and state privacy regulations such as HIPAA, the Computer Fraud and Abuse Act of 1986, GLBA, FISMA, the Electronic Communications and Privacy Act of 1986, and the Children's Internet Protection Act. In Europe, actions to monitor employee PCs for IP theft protection are curtailed by the privacy provisions of the EU Data Protection Directive.

- The convergence of cloud computing, big data, advanced analytics and data mining, social networking, intelligent connected devices, location-enabled tagging, and mobile technologies creates new vectors for privacy and intellectual property issues, some of which have yet to be identified. For example, pharma companies using cloud-based big data systems for clinical trials would have to consider steps to anonymize sensitive personal health information. Technology convergence also raises new concerns over data collection practices, consumer privacy, and cross-border data transfer protocols.

- Third-party cloud and big data systems create new classifications of sensitive personal information and new business processes, some of which have yet to be identified. Emerging information and process models highlight potential privacy and intellectual property ownership issues.

- Increasingly sophisticated, well-funded, and well-researched attacks are aimed directly at pursuing critical information such as intellectual property, trade secrets, business and manufacturing plans, R&D, market information, and access to mission-critical operations or national infrastructure.

The inability to manage and maintain an organization's multiple privacy and intellectual property obligations can result in data loss and privacy breaches, both of which have material implications on the brand and customer confidence.

5. **Cybersecurity risks.** As noted in the *Governance of Enterprise Security: CyLab 2012 Report* by Carnegie Mellon CyLab, businesses still have a lot to do in terms of addressing board-level oversight of activities related to cyberrisks. This includes undertaking key oversight activities related to cyberrisks, such as reviewing budgets, security program assessments, and top-level policies; assigning roles and responsibilities for privacy and security; and receiving regular reports on breaches and IT risks. At the operational level, the following developments increase a business' exposure to cybersecurity attacks:

   - Deployment and adoption of emerging technologies such as social networking, intelligent mobile devices (and the BYOD trend), cloud-based services, and big data systems present new attack vectors. Yet businesses fail to assess the impact on their existing risk posture and make the necessary adjustments to the corresponding security and risk protocols.

   - Perpetrators of cyberattacks are well-funded and well-researched, oftentimes targeting high-value digital assets. Attacks are often customized and employ multiple vectors, including very sophisticated socially engineered attacks through social networks. In many instances, these attacks are also very difficult to detect.

   - Businesses are becoming more globally interconnected, with complex ecosystems of business partners, some of whom are more vulnerable than others. Attackers are taking advantage of weaknesses in a business partner's information supply chain to penetrate the defenses of the business target.

- Organizational misalignment within IT operations, security operations, incident response and risk, and compliance makes multimodal attacks difficult to detect until it is too late. In many instances, the tools used to detect these attacks cannot scale to analyze and correlate security and operational information from multiple applications.

The inability of an organization to protect itself from cyberthreats could result in loss of customer confidence, fines and sanctions from regulators, actions from the plaintiff bar, and loss of a competitive business advantage from the theft or compromise of critical information and business services.

6. **BYOD and mobility strategy.** As noted previously, 46% of businesses already allow personally owned PCs as a primary work device. The proportion is no doubt higher when one takes into account the number of rogue devices proliferating within organizations that do not have official BYOD protocols. This global trend of employees using their own PCs, smartphones, and tablets for work continues to blur the line between work and personal activities. Privacy, data loss and IP theft, and eDiscovery are particularly tricky problems to address, especially when the device is decommissioned, lost, or stolen. The BYOD trend challenges existing risk and compliance programs in multiple ways:

   - Information governance, security, privacy, and acceptable use protocols must address the comingling of personal with corporate business data.

   - Applications that users download onto their devices need to be vetted and managed. Information-stealing malware continues to proliferate in the most popular app stores, opening up entry points for stealing credentials and valuable corporate data. The major app stores took steps to improve their security checks, but poorly written applications and intrusive data collection practices continue to be major issues.

   - Mobile hardware (especially tablets and smartphones) and mobile operating systems contain vulnerabilities that could be exploited to inject malicious code or exfiltrate valuable corporate data. Unsecured WiFi and cellular communication capabilities potentially expose these devices to proximity- and near-field communications (NFC)–based hacking.

   - The mobile ecosystem for security and compliance remains largely immature. Standards and practices are still evolving.

   The absence of an effective BYOD protocol limits employee productivity; at the same time, it exposes the organization to potential compliance violations and data loss.

7. **Supply/value chain risk.** Historically, supply chain risk and compliance focused on operational issues within an organization's complex ecosystem of suppliers, channels, distributors, and other business partners. Supply chain risk and compliance and risk management focused on demand management; supplier management, manufacturing, and logistics; regulatory and legal compliance (such as trade, export, environmental compliance, labor, and intellectual property protection); credit and financial compliance; quality assurance; and physical security (terrorism, piracy, and theft). The confluence of automation, intelligent connected devices, NFC technologies, geolocation tagging, machine-to-machine transactions, big data systems, and cloud computing adds another layer to existing supply chain risk and compliance management operations. Emerging supply chain challenges stem from:

   - Providing assurances on the integrity, provenance, security, and availability of the market data and automated business transactions across the physical supply chain (For example, Section 1504 of Dodd-Frank now specifies reporting provisions for extractive industries such as natural resources and oil and gas.)

   - Ensuring that information governance protocols associated with physical transactions are consistently executed by partners in the supply chain ecosystem

   IT outsourcing, BPO outsourcing, and cloud services extend the risk and compliance focus beyond the manufacturing- and retail-focused paradigm, to the information supply chain of all organizations, including those that provide information-centric business services (such as financial services, healthcare, and government).Here, the disciplines of supply chain, cloud computing, outsourcing, and vendor risk management converge. The challenges in this extended information value chain include:

   - Assurances on the integrity, provenance, and availability of the business processes and information associated with digital business services, as opposed to focusing solely on the documentation of physical goods transactions (For example, the United States–based law firm space outsourcing its legal review activities and U.S. medical practitioners using medical transcription services offered by business partners in India or the Philippines will want to ensure that these international partners have the appropriate security and privacy controls.)

   - Assurances on the identity and credentials of the actors and systems participating in the transactions

   - Risk assessment and audit of partners' and service providers' security, information governance, and compliance protocols

   - Management of risk inventories, as well as compliance and security protocols and dependency maps across the vendor and service partner ecosystem

- Harmonization and normalization of partners' protocols with the organization's internal standards

- Cost reduction and management of audit and reporting activities associated with business partners

Organizations that are unable to identify and manage risks in their supply and value chains are exposed to potential data loss and disruptions in their business services, in addition to actions from regulators, consumers, and investors that may result from violations in their compliance and privacy obligations.

8. **Building out infrastructure to enable situational awareness and predictive analytics.** The concept of situational awareness and predictive analytics is contingent on having the most relevant and accurate information about the organization's risk and compliance posture and funneling this information to the appropriate decision makers, in a timely fashion. Building out the underlying infrastructure presents organizational and technology challenges due to:

   - Silos of security, compliance, risk management, and IT operations disciplines within and across the partners' infrastructure. Normalization of critical information (such as risk inventories, data classification schemas, policies, and controls) can be cumbersome, time consuming, and prone to errors.

   - Contractual and regulatory mandates limit the type of security and risk information that organizations could share within their ecosystem of business partners. Data protection and privacy mandates also impose limitations on the monitoring of employee-controlled systems and devices.

   - Limitations on the ability of existing tools to scale and support collection, analysis, correlation, and visualization of dependencies across a massive array of data elements and processes. Today, organizations are in the early stages of leveraging big data systems to build out the architecture that could support these situational awareness and predictive analytics objectives.

   - The dearth of IT practitioners and data scientists with the requisite skills to develop, maintain, and use advanced security predictive analytics and risk management applications could slow down big data projects.

   - Building out the infrastructure for situational awareness and predictive analytics is a big-ticket and large-scale infrastructure project, and big data systems and cloud computing are well-positioned to deliver these capabilities. Big data projects for risk management and compliance compete with revenue generation and cost-saving initiatives where ROIs are much easier to quantify.

   Organizations that do not have situational awareness and predictive analytics capabilities are less prepared to detect and mitigate the more sophisticated threats in their IT networks and information supply chain.

9. **Aligning operational security with risk and compliance programs.** Business organizations typically have discrete, specialized teams for security operations, IT operations, IT audit, IT compliance, and incident response. Businesses struggle with aligning priorities and activities across these discrete disciplines because these specialized units often have their own best practices, policies, standards, and metrics. These discrete units also tend to deploy their own point products. Complexity is further compounded when geographical and business divisions are decentralized and operate independent IT organizations within each division. The by-products of this complex organizational and IT matrix are:

   - Silos of incompatible data, as well as conflicts, gaps, and inconsistencies in protocols and metrics
   - Unnecessary burden on the organization due to the duplication of effort, compliance conflicts, and inability to identify gaps
   - Lack of transparency on the true security, risk, and compliance posture of the overall organization and suboptimal allocation of resources

   Silos of incompatible data and processes hinder an organization's ability to effectively respond to potential vulnerabilities and compliance failures. As a result, an organization may experience a serious data security breach even after passing a scheduled audit. Organizations also struggle with aligning operational security with their risk management and compliance programs when the underlying GRC infrastructure is unable to scale to:

   - Provide a centralized system of record for policies, protocols, controls, and metrics
   - Deliver collaboration and orchestration of critical activities, as well as information sharing across the various departments
   - Analyze and correlate large data sets to enable situational awareness and predictive risk analytics

   Misalignment of operational security with risk and compliance programs leads to overlapping costs, inability to prioritize risk mitigation efforts, and undue burden on the relevant functional domains.

10. **Aligning business continuity and availability with risk management.** Businesses respond to potential risks in four ways: avoidance, reduction, transfer, and acceptance. When organizations determine that they can neither avoid nor transfer risk, they take steps to reduce their exposure. Business continuity and availability enable organizations to reduce disruptions to their ongoing business operations. Aligning business continuity and availability with risk management is challenging for most organizations because business continuity and availability are viewed as discrete disciplines, more closely aligned with storage operations than risk management. Specific hurdles include:

- Normalization of discrete data classification schemas, policies, requirements, controls, and metrics across the business continuity, storage, and risk management disciplines
- Mapping dependency across digital assets and processes, business impact analyses, recovery strategies and procedures, and compliance and risk management requirements objectives
- Integrating process and data across relevant functional applications to automate policy management, audit, reporting, and risk mitigation and remediation
- Tracking and managing incident response in real time, as well as implementing crisis management and response plans effectively
- Ensuring that business continuity and disaster recovery plans are updated to maintain alignment with the enterprise's evolving business objectives and priorities

Organizational misalignment between business continuity and risk management results in an inability to prioritize risk mitigation and business recovery activities. Organizations are unable to identify which business services are critical and must be protected and quickly recovered during a business disruption.

FUTURE OUTLOOK

The 10 GRC challenges highlighted all share a common theme: Process, information, and system silos limit transparency on policy and control requirements, as well as process and control gaps, conflicts, and critical dependencies. This handicaps the ability of an organization to gauge its true risk and compliance posture and creates bottlenecks and cost overlaps. These risk and compliance challenges are also interrelated and present potential adverse material impact to the business.

For many organizations, compliance, risk management, security, IT operations, and business stakeholders have become disconnected as a result of divergent priorities, reorganizations, acquisitions, and divestitures. Effective organizations are breaking down functional barriers and embedding risk and compliance awareness in their DNA during business transformation initiatives. They are doing this by moving away from regulation- or control-centric value propositions into approaches that pragmatically integrate risk and compliance with the business and IT operations domain. Effective businesses are executing these strategies by leveraging processes and technology in tandem with information and organizational governance to:

- Develop a system of record for key standards, protocols, and classification schemas
- Understand dependencies across the business and GRC domains
- Develop standard processes and utilize tools to automate cross-functional collaboration in key activities such as policy management, compliance management, risk assessment, audit management and reporting, incident

response and crisis management, business continuity management, supply chain and vendor risk management, cyberrisk management; situational awareness, and predictive analytics

- Enhance the effectiveness of existing compliance, security operations, risk remediation and mitigation, and business value creation activities by using visualization and analytics to funnel timely and accurate information to the relevant decision makers

EMC Solutions for Enterprise Governance, Risk, and Compliance

As businesses adopt best practices and coordinate historically siloed risk and compliance programs, EMC is facilitating this process through the following:

- EMC technologies to automate risk and compliance activities. With RSA Archer as the cornerstone, EMC offers out-of-the-box integration with information governance, security, IT operations, and storage assets.
  - RSA Archer offers modules for enterprise GRC, audit management, business continuity management, compliance management, enterprise management, incident management, policy management, risk management, threat management, vendor management, and performance management. Customers can choose the module that best fits their immediate risk and compliance needs, or they can build a custom Archer GRC application.
  - The out-of-the-box integration of RSA Archer GRC with RSA Security Analytics (NetWitness, RSA enVision) and RSA DLP and associated reference architectures delivers advanced security risk intelligence, advanced threat management, and compliance management and facilitates the alignment of IT security operations with risk and compliance programs.
  - The RSA Archer integration with EMC Network Configuration Manager, EMC Storage Configuration Advisor, VMware vCenter Configuration Manager, and EMC Data Protection Advisor facilitates audit, change, and compliance management of the IT infrastructure. In addition, the integration also serves as a foundational element for enabling visibility in IT environments, enabling IT risk management, and aligning business continuity and availability with risk management programs.
- EMC and RSA complement the out-of-the-box integration from EMC technologies by delivering deployment and implementation best practices and reference architecture solutions. These solutions allow the customer to deliver risk and compliance capabilities through physical, virtual, and cloud-based delivery models; at the same time, they enable consistent management and deliver a unified view of the enterprise's risk and compliance posture across these hybrid environments.

- EMC Consulting Services help customers with the planning and design, deployment, and implementation of their enterprise risk and compliance program. The service offerings are designed to enable customers to choose the GRC maturity path that best fits their needs. EMC GRC Advisory Services help organizations effectively adapt their GRC programming to the changing risk profile of their operations.

  - GRC Program Strategy and Strategic Planning services assist clients in assessing and defining the scope of their GRC programs as well as in assessing the maturity of existing discrete compliance and risk management programs.

  - GRC Program Development services assist clients in developing a program for understanding their risk profile, including defining risk hierarchy, appetite, and risk ratings as well as developing the appropriate risk reporting framework, metrics, and risk remediation process and plan.

  - GRC Program Management Optimization services enable clients to gain efficiencies in managing, monitoring, and measuring the performance of their GRC programs by supporting integration of GRC processes, policies, and controls with RSA Archer.

CHALLENGES

Business organizations and their technology partners, like EMC, are collaborating to successfully overcome common challenges to an effective enterprise GRC program. These hurdles include:

- **GRC program maturity.** Organizations that have not adopted industry best practices and standards for their specific functional disciplines will have a steep learning curve.

- **GRC technology maturity.** Discrete functional disciplines are using semimanual solutions or standalone solutions to address their unit's risk and compliance requirements. These solutions do not have the ability to scale and orchestrate risk and compliance activities across functional disciplines.

- **Organizational resistance to change and silo mentality.** The absence of shared responsibilities, goals, and incentives impedes organizational alignment.

- **Budgets.** Innovative risk and compliance initiatives compete with revenue-focused business transformation projects for budget dollars. Internal competition is particularly pronounced in investments for big data systems and cloud computing.

CONCLUSION

Effective businesses view the confluence of business, technology, legal, and regulatory developments as an opportunity to address the gaps and weaknesses in their existing risk and compliance programs. These businesses focus on leveraging their investments in a GRC platform to:

- Enable organizational alignment across the GRC functional disciplines with business operations
- Leverage the integration across functional disciplines in IT operations, security, and business operations to reduce the compliance and audit burden
- Leverage the integration across functional products in combination with emerging technologies to enable capabilities for addressing new sources of risks, security, and compliance challenges (These include capabilities for aligning cyberrisk management, enhancing situational awareness and predictive analytics, and aligning security operations with risk management as well as business continuity with risk management.)