



ENTERPRISE GOVERNANCE, RISK AND COMPLIANCE: A NEW PARADIGM TO MEET NEW DEMANDS

Executive Summary

In our increasingly globalized business environment, economies and enterprises are steadily becoming interrelated. Yet many key functions and departments that deal with related information and business processes remain siloed. As competition escalates, as organizations become more dispersed, and as regulations increase in number and complexity, risk inevitably grows. So, too, does the demand—from markets, regulators and customers—for increased accountability.

The answer is to bring governance, risk management and compliance together in an integrated program where policies, data and controls are strategically managed and visible throughout the enterprise. An enterprise governance, risk and compliance (eGRC) strategy, supported by a common technology platform, creates consistency and transparency, enables collaboration, fosters operational efficiencies, and ensures the continuity and success of the business.

eGRC is not just another assemblage of solutions to address the same old problems. Rather, it is an innovative and multifaceted approach to a new paradigm, where risk management and compliance issues are seen not as isolated concerns but as closely related strategic initiatives with a direct impact on business objectives. These concerns, therefore, require the attention and influence of governance, which ultimately is responsible for business growth and performance.

I. THE EMERGENCE OF EGRC AS A BUSINESS IMPERATIVE

The emergence of eGRC as a strategy for protecting the enterprise from excessive risk while removing barriers to growth is the result of a number of factors, including:

- Demands on corporate governance
- Multi-faceted risk environment
- Growing regulatory requirements
- Disappearing boundaries in the hyper-extended enterprise

DEMANDS ON CORPORATE GOVERNANCE

Governance refers not just to the people in charge of a business but also to the culture, policies, processes, laws and institutions that define the structure by which companies are directed and managed. Governance affects how the company addresses everything from long-term strategies to day-to-day operations. Ultimately, though, when things go wrong, it's not the culture or the policies that are called to task, but the executives and the board of directors. This is the all-important area of accountability—the issue of whether internal and external constituencies trust that the company is doing everything it can to mitigate risk and enable growth.

The media, traditionally more focused on rooting out dirty politicians, now are hot on the trail of companies that fail to protect sensitive information. Because of this media attention, the increasingly complex regulatory environment, and the devastating effects of a data breach, executives and board members are more closely attuned than ever to how their businesses do business. This is certainly not a bad thing, but it means that those in governance need accurate, timely information about the company that is both broad and deep. Only then can they make decisions to stave off unnecessary risk, ensure compliance and minimize the chances and impacts of shareholder litigation and regulatory penalties.

MULTIFACETED RISK ENVIRONMENT

Risk is one reason why board members are becoming more involved in the company, but risk in and of itself is neutral. As anyone with a 401(k) knows, some risk is well worth taking. Risk, then, is merely the effect of uncertainty on business objectives, while risk management describes the coordinated activities undertaken to direct and control the organization in taking advantage of potentially lucrative opportunities while managing the potential for negative effects. Knowing what could go wrong makes it easier to choose the course that makes things more likely to go right.

The increase of risk in today's business environment comes from a number of areas, from the dynamic and global nature of business to the growth in competition and litigation, to geopolitical unrest in regions that companies may not have invested in 20 years ago. With a more complex risk environment, a more holistic approach to risk management must become a priority. For every key performance indicator defined to measure success against strategic objectives, there are several corresponding key risk indicators that may impact the likelihood of hitting those goals.

GROWING REGULATORY REQUIREMENTS

Compliance refers not only to the act of adhering to regulations but also to an organization's ability to demonstrate and sustain adherence to regulations—and not just externally imposed laws and regulations, but also internal corporate policies and procedures. Adding to the challenge are ever-increasing regulatory requirements, more serious penalties for noncompliance, more assertive (and global) regulators and a more informed public.

Furthermore, managing compliance becomes increasingly difficult as much of the world moves toward principle-based regulation, which focuses on outcomes rather than checklists of requirements. Organizations are not told how to comply but rather what they have to achieve, which includes the ability to clearly document their compliance program and provide evidence of its effectiveness. There are multiple ways to achieve the desired outcome, and organizations need to chart their plan of action for reaching those goals. This requires integration of risk management practices with compliance—a new paradigm for many businesses.

DISAPPEARING BOUNDARIES IN THE HYPER-EXTENDED ENTERPRISE

Today's business is not a self-contained entity but instead represents an intricate, far-reaching web of business relationships. Information is exchanged with more constituencies in more ways and more places than ever before. Technologies such as cloud computing, virtualization, social networking, mobile devices and VoIP services—along with outsourcing—mean that the traditional boundaries of an enterprise are disappearing. With all this cross-pollination of services and information, it can be difficult to define where one enterprise ends and another begins. This makes fertile soil for unwanted risk.

Managing hundreds or thousands of business relationships across the globe is a daunting task. Organizations are burdened with assessments related to quality, facilities, environmental management, health and safety, security, privacy, workflow support and employment practices across these relationships. Still, organizations must validate that members of their extended enterprise (including business partners, contractors, consultants, outsourcers and suppliers) are complying with laws, meeting their social responsibility practices, and operating in a way that does not introduce unnecessary risk.

New technologies create as many risks as they do opportunities. For example, today's mobile consumer market has a direct impact on an organization's delivery of products and services, and creates new expectations of connectivity and fast, seamless and consistent experiences across various touch points. At each touch point, there is an opportunity to strengthen or ruin the customer relationship, depending on how secure and successful the interaction is—and how well the organization is able to protect its customers' privacy when so much more personal information is available for the taking.

II. ENTERPRISE DOMAINS MOST AFFECTED BY EGRC

Four key domains within an organization are most directly involved in eGRC. They include IT, Finance, Operations and Legal. In each of these domains, leaders must manage numerous policies around critical business processes and multiple regulations, and to each process, a control must be applied. Across the four domains, there is typically a significant amount of overlap and redundancy within the core processes of Policy, Risk and Compliance Management. For example, different domains often deal with the same policies related to the same processes and regulations, and apply the same controls. Unfortunately, they are not talking to each other, resulting in a great deal of waste and inconsistency.

With an eGRC strategy in place, these domains would collaborate on their requirements, enabling them, as appropriate, to apply the same control to different regulations. A hospital, for example, could use the same control to ensure compliance with both PCI and HIPAA. Authentication alone, as a control, applies to about 16 different regulations. It would be difficult and costly to manage these regulations manually, but eGRC enables a “one-to-many” process that reduces redundancy and repetition, improves efficiency and consistency, and keeps everyone aware of what's going on.

Consider the following risk and compliance issues faced within each domain:

Information Technology. The IT department has typically focused on technical risk and compliance challenges, attempting to keep hackers, viruses and worms at bay while maintaining systems in a state of recovery should a disaster strike. Today, with the onslaught of regulations, the IT department is struggling to build its own legal acumen to comply with increasingly complex laws and regulations, as well as managing policies that map to specific regulations and tying those policies to controls. By taking a systematic approach, IT can eliminate its own silos.

Finance. In the early years of Sarbanes-Oxley, Finance executives struggled to define internal controls, assess those controls, survive (let alone respond to) internal and external audits, defend financial performance results to stakeholders, maintain segregation of duties and ensure the accuracy and integrity of financial reporting. Though demonstrating Sarbanes-Oxley compliance has become a much more streamlined process for many organizations, finance executives are still challenged to stay abreast of financial risk and internal controls over the full range of accounting processes.

Operations. Because Operations is where products are made, services are delivered, employees are managed and customer relationships are maintained, this domain is on the front line of risks that could harm the business. From missed delivery schedules to missed forecasts, from production problems to supply chain breakdowns, from internal policy violations to customer touch point issues, there are innumerable potential trouble spots that COOs must monitor.

Legal. Responsible for ensuring adherence to external laws and responding in the event of a violation, Legal knows only too well how compliance and other risks can impact the business. Yet because risk is everywhere and regulations touch all business units, Legal can't be proactive and comprehensive in its work unless it has the ability to audit compliance efforts throughout the enterprise and to identify which areas present the greatest risk of legal action against the company.

Because these roles tend to work in silos and often lack a sustainable strategy for cooperation, they take varied approaches to ensure compliance and minimize risk. As a result of these redundant and inconsistent efforts, resources are easily drained, accountability and information-sharing (and therefore visibility) are lacking, and it is extremely challenging to correlate and prioritize the most pressing issues.

III. THE RESULTS OF AN OUT-DATED APPROACH

Instead of treating each risk and compliance issue as an individual problem, organizations must look for a common approach to managing risk and compliance across the hyper-extended enterprise. Organizations that don't achieve this level of collaboration are paying a significant cost in terms of wasted resources, increased complexity, decreased flexibility and, ironically, even greater exposure to risk that threatens business performance and growth.

We explore each cost briefly:

- Wasted resources.** Instead of prioritizing how resources can be leveraged to meet a range of needs, organizations tackle issues one-by-one, resulting in varying processes, systems, controls and technologies. The excessive time and expense required to do this takes the focus away from business initiatives that can improve the bottom line.
- Increased complexity.** Inconsistent risk and compliance approaches introduce greater complexity to the business environment and with complexity comes increased inherent risk. When controls are not streamlined and managed consistently, there are more points of control failure and compliance gaps. Further-

more, inconsistency in controls means inconsistency in documentation of risk and compliance, which can further confuse the organization, regulators and business partners.

- **Decreased flexibility.** When an organization is spinning multiple risk and compliance plates, its ability to respond to other issues is compromised. The organization ends up doing a substandard job on the plate-spinning and sees its own business performance suffer because it is less able to respond to emerging opportunities.
- **Greater exposure.** With the focus on what is immediately at hand and not on what the business needs to protect itself in the long run, an organization will find itself facing more present threats rather than fewer. Duplication of processes and gaps in coverage are bad enough, but when they aren't visible at the governance layer, the business is at the brink of exposure to serious risk.

IV. THE PARADIGM SHIFT TO EGRC

Clearly, organizations can no longer afford to focus on risk and compliance issues separately. A new paradigm is needed—one in which multiple business domains work together under a unified framework to ensure that processes and systems, as well as partners and employees, behave as a cohesive, well-governed unit.

Organizations must take a deep look into their long-term vision and plan today for the future risk and compliance challenges. While no organization can eliminate all the complications of a rapidly advancing and transforming world, the better able it is to proactively identify and address pressing issues, the more likely it is to safely navigate the waves of change and emerge successful on the other side.

GOALS OF AN EGRC STRATEGY

At its core, an eGRC strategy aligns people, processes and technologies across IT, Finance, Operations and Legal domains. Because no company has a Chief eGRC Officer, what's needed is a cross-domain steering committee that comprises the head of compliance, the general counsel, the CSO or risk officer, the head of audit and the controller's office. This committee would typically report to the finance head or the Chief Administrative Officer and its success depends on how well stakeholders engage to share information and integrate their efforts for a holistic view of governance, risk and compliance across the enterprise.

Senior executives must understand and acknowledge the interrelationships among governance, risk and compliance—and be committed to having these processes working in harmony in order to increase collaboration, reduce uncertainty in business and produce more predictable results. It is critical, therefore, to gain consensus on the goals of an eGRC program, which are as follows:

- **Accountability.** Organizations require a system of accountability where executives can see the status of issues, events, incidents and unresolved findings, and hold individuals accountable for their resolution. Big-picture visibility of eGRC is necessary, along with the ability to drill down into specific areas.
- **Sustainability.** Organizations demand a sustainable process and infrastructure for ongoing governance, risk and compliance processes that are becoming more plentiful and complex. As business is changing rapidly, point-in-time assessments are no longer good enough by themselves. Business is changing minute by minute, requiring that organizations address eGRC issues collaboratively and continuously.
- **Consistency.** Organizations need tools that force them to be consistent in their methodology and reporting so they can compare apples to apples. Without consistency, there is no way to effectively prioritize issues and resources. eGRC

How an eGRC Platform Enables Risk-based, Business-aligned Internal Audit

In an effort to provide more value to the business, audit's focus is shifting from compliance to risk, so instead of looking for control failures, the function is being preventative, attempting to keep failures from occurring. Now that auditors are being challenged to validate structure, processes, policies, and controls across governance, risk, and compliance domains, audit is becoming a key player in eGRC initiatives. This means that not only has the scope of work changed, but the nature and the tools have changed as well. While a learning curve is required, ultimately eGRC offers significant benefits for internal audit.

Currently: Auditors have to piece together decentralized documentation captured in multiple systems. They lack visibility into existing risk assessments, and audit plans themselves lack the flexibility to react to emerging risks and business concerns. There also is an inability to track the status of risk mitigation efforts resulting from audit findings. As a result, audit struggles to focus on issues most critical to the business.

With an eGRC Platform: Auditors can coordinate information, priorities, and objectives among audit, risk, and compliance teams, and ensure that the audit plan is aligned with the organization's priorities and business objectives. External auditors can securely self-serve the information they need, and business units can manage and track their own findings and remediation efforts within the same repository as the audit department. With a consistent audit process and methodology supported through one centralized system, the organization benefits from higher-quality audit projects, more productive and efficient auditors, and a reduced risk of fines, loss events, and operational costs from unresolved findings.

ensures that every critical domain and function in the organization knows the big picture and understands their role in it.

- **Efficiency.** Redundant assessments and audits looking for similar information for different purposes are wasting resources and preventing lines of business from operating as productively as possible. eGRC aims to ease this burden by leveraging common processes, assessments and information across the enterprise.
- **Security.** In today's uncertain business environment, senior management wants peace of mind that any threats to executing on business strategy are being kept at bay. Security oversight aims at understanding and modeling various threats, likelihoods and business impacts to select and prioritize controls in order to bring systems and information in line with acceptable levels of risk tolerance.
- **Transparency.** Business demands transparency across key performance and risk indicators so it can monitor the organization's health, take advantage of opportunities and avert or mitigate disaster.

V. A PLATFORM APPROACH TO EGRC

Organizations frequently rely on a document-centric, paper-based approach to risk and compliance management, rarely attaining sophistication beyond electronic documents and spreadsheets. Aside from being error-prone and inefficient, this approach makes it difficult to share information, thereby reinforcing silos. Today's business requires a technology architecture that integrates with other systems and provides for a cohesive and common eGRC platform. This platform should tie into enterprise applications and infrastructure, consolidating the information necessary to manage risk and compliance throughout the organization.



Requirements for such a platform include:

- **Centralized views.** A central view of risk and compliance activities provides a single lens through which stakeholders can identify threats early and prioritize issues, as well as improve efficiencies by applying a single process to multiple regulations.
- **Automation.** Through automation, organizations achieve continuous risk and controls monitoring as opposed to the point-in-time spot checks of the past. Technological capabilities required include advanced risk analytics and modeling, automated controls tied to business rules engines, advanced content and process management capabilities, and embedded eGRC control points.
- **Integrated systems.** Multiple point solutions that span different areas of the infrastructure are costly to manage, fail to deliver a holistic view of the enterprise and cannot correlate analysis to provide reliable conclusions. Integration enables management and reporting across the enterprise. (See “Information Integration and Business Context” below for more on this requirement.)

How an eGRC Platform Enables Better Business Continuity Planning

Risk management in the realm of business continuity goes well beyond typical (and still quite serious) threats such as data breaches, potential litigation, production snafus, and customer and competitor issues. The very ability of the business to operate is at stake and the current tools in use to respond to business continuity issues are often insufficient. Furthermore, plans are not always updated, so they are based on old information formulated in a different context. Risk has to be classified based on impact and likelihood, and plans must be regularly updated.

Currently: As with audit, business continuity and disaster recovery teams are stymied by decentralized, static documentation captured in multiple tools and inflexible systems. They lack visibility not only into plan status, approvals, review dates and testing, but also into emerging IT and business risks that can impact their plans. Because of this, there is uncertainty over which processes, technologies and other infrastructure components need to be recovered first, and how to provide real-time response information to people who need to know where to go and what to do in a crisis.

With an eGRC Platform: Employing an eGRC platform, organizations can better coordinate information, priorities and processes among business continuity, disaster recovery and crisis teams, ensuring that contingency planning is strategic (i.e., aligned with the organization's priorities and business objectives). Business-relevant reporting is generated automatically from day-to-day plan maintenance, so plans are accurate, relevant and accessible. Ultimately, an eGRC platform enables accelerated and appropriate response to crises, which reduces the impact of an event on revenue, brand image, market confidence and customer loyalty.

– **Flexibility.** An eGRC platform must be adaptable in order to evolve as the business evolves. Furthermore, business users must be able to make changes and build out applications to solve business problems without relying on costly, time-intensive custom development. Every business has different risk management and compliance requirements, so the eGRC platform must be tailored to an organization's specific needs and structure.

INFORMATION INTEGRATION AND BUSINESS CONTEXT

Organizations have an extraordinary range of data that is relevant to risk and compliance management. However, in many cases this data is scattered across multiple tools and systems, making it extremely difficult to put risks, threats, incidents and compliance deficiencies into business context and to prioritize the response based on what is most significant to the organization.

Examples of relevant risk and compliance data include, but are not limited to, the following:

- Risk analytics
- Loss events
- eDiscovery
- Configuration scan results
- Security event logs
- Sensitive data discovery
- Document and records retention data
- Threat intelligence
- Vulnerability scan results
- Emergency notification call chains
- Asset and supply chain management data
- Customer and partner profiles
- Accounting and HR information

In order to pull in such diverse types of information from a multiplicity of sources, including proprietary solutions, an eGRC platform must be vendor-neutral and able to identify and correlate disparate data from all parts of the enterprise.

VI. DEVELOPING AN eGRC STRATEGY ROADMAP

The web of stakeholders with varying requirements for governance, risk management and compliance often results in a complex tug-of-war with opposing priorities. But efficiency can be achieved through the definition of common processes and technologies that various parts of the organization can utilize for their individual requirements, as well as for collaboration and sharing. A successful eGRC strategy, therefore, is one that has a symbiotic influence on stakeholder roles and their common requirements.

Any organization looking to advance their risk and compliance efforts from tactical to strategic and from isolated to collaborative should begin by defining a strategic roadmap. An eGRC strategy roadmap is a multistage process that begins by identifying all of the business processes throughout the enterprise that fall under the eGRC purview. This is no small task as it requires determining the process owners and subject-matter experts, and getting those individuals together to create consensus over pain points, workflow, dependencies, complexity, the desired future state and existing (and lacking) supporting technologies. Once this is completed, each business process must be analyzed to identify opportunities for automation and for eliminating redundancies (and there will be many of both).

The results of these analyses are then delivered to a cross-functional steering committee (discussed earlier in “The Paradigm Shift to eGRC”), which is charged with defining the organization's eGRC program: its vision, goals, components, stakeholders and underlying technologies. Through this leadership team's discussions, a tactical, phased approach to implementing the program emerges, along with a strategy for how it matures to its desired state. This plan must take into consideration both dependencies and redundancies to ensure an effective implementation.

The EMC Approach to eGRC

EMC Corporation (www.emc.com), the world's leading developer and provider of information infrastructure technology and solutions, offers a rich portfolio of products and services for managing enterprise governance, risk and compliance (eGRC) across IT, Finance, Operations and Legal domains. RSA, The Security Division of EMC (www.rsa.com), delivers a foundational element in this portfolio—the RSA® Archer™ eGRC Suite. This set of automated, integrated solutions built on a common technology platform enables organizations to centrally manage policies, controls, risks, assessments and deficiencies across the enterprise, and to report on the organization's risk profile and compliance posture through real-time executive dashboards.

CONTACT US

To learn more about how EMC products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller—or visit us at www.EMC.com

It is important to note that eGRC isn't just a technology buy. The success of an eGRC program depends on how well organizational stakeholders work together to share information and integrate their efforts to enable a holistic view of risk and compliance across the enterprise. Therefore, it is a combination of people, processes and technologies that all must be aligned behind a common goal and commitment. To sum up, the eGRC strategy roadmap includes these key phases:

- **Inventory.** Take an inventory of individual risk and compliance processes across the organization. This requires that the organization step outside of internal silos and collaborate on a range of risk and compliance issues.
- **Analysis.** Identify which parts of the organization have strong processes and where processes can be improved, specifically by introducing automation and eliminating redundancy.
- **Goal-setting.** Outline where you want to be in three years and model the ideal eGRC strategy and implementation approach. Think outside the box so you are not locked into current approaches and processes—many of which may be failing.
- **Planning.** Build the plan to achieve the desired eGRC strategy and implementation approach. Identify the biggest eGRC issues and address the most visible and inefficient issues first. Think big picture, but start in areas that can provide quick wins.

Of course, prioritization of risk and compliance activities must be decided at the business level to ensure maximum impact and sustainability. An eGRC strategy roadmap requires executive buy-in and support, which provides endorsement of the effort and overcomes obstacles of siloed entities wanting to work independently and do things their own way. As with any new paradigm, implementing eGRC requires a committed change management program.

VII. CONCLUSION

One thing is certain: risk and compliance burdens are not going away. Government regulators continue to influence control upon organizational practices through tighter regulation, and business partners are requiring stronger controls within their relationships. The globalization of business introduces significant risk with more points of vulnerability and exposure. The time is now for organizations to define and implement an eGRC strategy that drives accountability, sustainability, consistency, efficiency, security and transparency. Selecting the right technology vendor that provides for enterprise-level control and integration of risk and compliance is a critical step that organizations should not take lightly.

That said, organizations face an array of technologies to consider as the foundation of their eGRC program, and the process of selecting the right vendor to build a sustainable eGRC program can be overwhelming. When evaluating IT vendors, organizations should consider the range of risk and compliance requirements impacting the business and select a vendor that has the strongest integrated solution to manage these requirements on a consistent, ongoing basis. The right technology platform lays a strong foundation for an effective eGRC strategy.

EMC2, EMC, the EMC logo, where information lives, Archer and RSA are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners. © Copyright 2010 EMC Corporation. All rights reserved. Published in the USA. 09/10 EMC Perspective EGRC WP 0910-EMC