



Enabling Cost-Cutting Initiatives with Governance, Risk and Compliance Management Technology

Executive Summary

As a result of the financial crisis beginning in 2008, companies are faced with an ongoing dilemma: reduce costs now while maintaining an appropriate risk management structure and preparing for the impending increase in regulatory demands. Organizations must look to improve operational efficiency in enterprise governance, risk and compliance (eGRC) initiatives to meet current fiscal concerns while providing a framework on which to build a rigorous eGRC program. eGRC management technology can drive cost savings, improve process efficiency and deliver the needed platform to meet regulatory and risk demands today and in the future.



The Security Division of EMC

The Issue

Faced with some of the greatest challenges in history, companies are focusing on cutting costs and more stringent fiscal management. Regardless of industry, organizations are reassessing investment budgets, reducing staff and implementing other measures to reduce operational expenses across all business disciplines. The issue is where and how deep to cut without impacting competitiveness or elevating risks beyond a level that is tolerable.

How Companies Are Addressing the Issue

Businesses are conducting cost-benefit analyses across the board, and a critical part of the analysis is understanding risks associated with cost-cutting measures. Additionally, compliance cannot be lost in the shuffle. Deciding where and how much to cut must be balanced with many factors affecting risk and compliance.

Whether the company is looking to reduce inherent business risks or exploit an advantageous business initiative while managing risks, risk management techniques and technology can be used to better understand the impacts of cutting costs. For example, risk management processes and supporting technology can be used to identify areas of concern and exposure during the financial analysis of cost cutting, and these processes and technologies are themselves candidates for improved operational efficiency. The bottom line is that a stronger risk perspective due to improved risk data leads to better business decisions.

Companies are also weighing the impact of the impending regulatory focus as a result of the financial crisis. Organizations must look to improve operational efficiency in governance, risk and compliance initiatives to meet today's fiscal concerns while managing risk taking and return in a complex environment. Compliance management technology can drive cost savings while delivering the needed platform to meet regulatory and risk demands now and in the future.

The Impact

Risk Management can support an overall cost management strategy in many ways. For example, a well-run risk management process can aid in determining the right balance of controls that must be implemented to mitigate reductions in staff or other identified areas. Consider this: Within Information Technology, some organizations are deferring investment in newer technologies and reducing staff. Understanding the risks associated with these reductions and designing controls based on these risks will diminish the likelihood that reductions will affect business-critical functions. The company must also weigh the immediate benefits of deferring investment with the long-term impact of a less agile or stable environment. A risk monitoring process should be implemented to assess control effectiveness, monitor impact to the organization and minimize residual risks associated with cost-reduction efforts.

Faced with budget freezes and cuts, many organizations are deferring eGRC technology investments. This approach can backfire, however, because inefficient, manual, duplicative and siloed processes cost the organization significant time and money. Spreadsheets, Word documents and custom tools get the job done—but at what cost?

eGRC solutions that streamline policy management and measurement, reduce the number of controls needed to comply with regulatory requirements, and automate and improve control monitoring and reporting will enable organizations to reduce costs, improve operational efficiencies, and provide a framework on which to build a governance, risk and compliance program.

Maintaining the status quo of stovepipe GRC ultimately reduces a company's ability to see across the organization and have transparency and accountability in the entire risk management spectrum. This can be seriously dangerous in today's complex and turbulent business environment.

“Analysis that previously required months of research can be done in minutes and in much greater detail, leading to a 97.5% cost reduction in the risk analysis process.”

Mandy Andress, MassMutual¹

* 1 Greenemeier, Larry. “MassMutual Gets Control of Its Security Data.” InformationWeek 17 Sept 2007.

Understanding and Quantifying Enterprise GRC Costs

The guidelines and questions below are designed to assist companies in better understanding their current costs so they can identify opportunities for cost savings and improving operational efficiencies. Answers to these questions can be used as a basis for return-on-investment (ROI) calculations and cost justifying eGRC technologies.

eGRC initiatives can be grouped into three categories:

- **Content Acquisition and Development** . Researching regulations, risk management approaches and control frameworks, along with developing and mapping policies to risks, corporate objectives, regulations, and controls for auditability and measurement.
- **Governance and Policy Management** . Creating and managing governance and risk management policies and controls, along with communicating policy requirements to the extended enterprise.
- **eGRC Management and Reporting** . Auditing policy adherence and measuring the current state of the environment against defined controls, along with reporting and analyzing results and trends and determining root cause and remediation needs for compliance issues, losses and incidents.

Companies can use these categories as a framework for answering questions to uncover inefficiencies and identify opportunities for costs savings.

Content Acquisition and Development

- Does the organization have an enterprise approach defined for policy management?
- Does the organization have a complete risk taxonomy that shows the relationship of risks to each other and to business performance and regulatory requirements?
- Does the organization have good risk intelligence on both the internal business environment as well as external environments that the business operates within?
- How has the organization established and monitored key risk indicators and mapped them to key performance indicators for the business?
- How much time is spent researching business and regulatory requirements and identifying controls to manage associated risks?
- When were the company's policies last analyzed against a set of multi-regulatory requirements and industry standards?

- How many resources (dedicated and non-dedicated) are responsible for keeping up with changing regulations and frameworks and incorporating changes into policies and controls?
- Are resources expected to develop control content as a side job, or is there a defined process to enhance and refresh control documentation on a regular basis?
- Is control documentation spread across the organization with little consistency in format and detail?
- Are there areas (policy domains, technologies, processes, roles) that the organization needs to address from a risk perspective but does not have the time or resources to research and document controls?
- Are new technologies researched and documented from a control perspective?

Governance and Policy Management

- How much time is spent creating and managing governance and policies?
- How many people (dedicated and non-dedicated) work on policy creation and management?
- How much time is spent on managing and monitoring risks, including risk and control assessments for varied business requirements?
- Has the organization established a maintenance infrastructure to leverage knowledge enterprise-wide to design controls that are relevant and practical for the business?
- Does the organization have a mechanism to facilitate collaboration on risk management decisions, policy and control documentation?
- How much time and effort does it take for management to review and approve policies before distribution?
- How much time does it take for the average employee to research corporate standards to determine control requirements for projects, business initiatives or operational processes?
- Does the organization have an established system of record that centralizes control documentation for ease of communication and distribution?

eGRC Management and Reporting

- How much effort is spent on assessing and auditing systems and processes against corporate policies and regulatory requirements?
- How much time does it take to assess risks associated with the findings of these assessments and audits?

- Can potential risks be presented in a consolidated fashion leveraging compliance efforts?
- How much effort is spent on monitoring and reporting governance, risk and compliance levels across the organization?
- How many duplicative audits and risk assessments are being performed by siloed groups to meet regulatory or business compliance requirements?
- How many people are dedicated to performing assessments and compiling eGRC reports?
- How many business systems are queried to gather risk and control compliance information? How long does it take to organize and consolidate this information?
- How long does it take to compile information for internal or external audits?

Cost-cutting efforts should focus on areas that can be more efficiently handled by automation or external sources so internal staff can spend their time analyzing and responding to business needs. Objectives should be set to:

- Decrease the time and costs associated with researching and documenting risk management requirements
- Formalize risk management processes to ensure control coverage based on business and regulatory requirements
- Improve consistency and coverage of controls
- Improve control awareness with employee training and education
- Reduce costs for policy creation, management and communication
- Reduce costs and improve the quality of ongoing risk management
- Automate the distribution, collection and reporting from surveys and other assessments for procedural controls
- Automate the collection of configuration data from systems and platforms for risk and control monitoring

The Bottom Line

Organizations are faced with an ongoing dilemma: reduce costs now while preparing for the impending increase in regulatory demands and managing risk in a complex business environment. With these challenges comes a tremendous opportunity to respond with innovation rather than knee-jerk reactivity. Business must think strategically and establish a foundation on which

to build a longer-term risk and compliance program while immediately solving pressing requirements.

eGRC technology should be used to address this dilemma and replace existing inefficient tools and processes. This technology must be flexible and designed with business users in mind, enabling them to capture new information, modify workflow, integrate with other enterprise systems and deliver real-time reports without relying on costly, time-intensive development processes.

Organizations with a solid eGRC approach, supported by the right technology, are better suited to manage a lean organization. An improved governance process with strong corporate policies that are managed, communicated and measured for adherence allows businesses to manage risks and demonstrate compliance more cost effectively.

To make up for a leaner workforce, companies must leverage knowledge enterprise-wide. This requires improving control management processes, facilitating collaboration and distributing responsibilities to critical personnel with the ability to impact the full organization. Businesses must utilize automation to better manage, communicate and measure policy adherence and implement and monitor controls. By minimizing manual, duplicative, time-intensive processes without the expensive overhead of internally developed solutions, organizations will reduce costs and improve operational efficiency. eGRC solutions are critical to this approach.

“There’s a perception if budgets are cut, innovation goes with it. I would say it’s just the opposite. I would say we have to be more innovative and adopt best practices with an eye toward saving operating costs as we do it.”

Jim Routh, DTCC²

* 2 Mimoso, Michael S. “Recession Forces Security to Measure and Prioritize Risks.” Information Security February 2009.

About the Author



Steve Schlarman is an eGRC Solution Manager for RSA, The Security Division of EMC. With deep compliance, security, audit and IT management expertise, Mr. Schlarman is responsible for product design and architecture for RSA Archer eGRC Solutions, in addition to content management processes specific to the Policy and Compliance Management solutions.

Prior to joining RSA, Mr. Schlarman was the Chief Compliance Strategist for Brabeion Software where he led overall product strategy, product management and content management. Before Brabeion, he was a Director in PricewaterhouseCoopers' Advisory Practice, focusing exclusively on information security consulting and auditing. During his tenure at PwC, Mr. Schlarman led a wide range of security and compliance engagements, including security strategy, security policy development, audits, penetration studies, Sarbanes-Oxley preparation and computer crime investigation.

Mr. Schlarman holds both CISSP and CISM certifications and is an RSA Archer Certified Consultant.



The Security Division of EMC

www.rsa.com

©2010 EMC Corporation. All rights reserved.
EMC, RSA and (see list) are registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other products or services mentioned are trademarks of their respective owners.

CCGRC IB 1010