The RSA GRC Reference Architecture

Abstract

This paper is a primer on the RSA GRC Reference Architecture – a visual representation of the GRC framework needed within an organization to meet today's governance, risk and compliance needs. The architecture provides a starting vision of how an organization should view GRC, its guiding principles and its final objectives.

Date: June 2013

Contents

Introduction to the RSA GRC Reference Architecture 3
GRC's Guiding Principles 3
The RSA GRC Reference Architecture 5
Business Optimization 6
The Value Layer 6
The GRC Core 6
Governance 7
Risk 7
Compliance 7
The Organizational Stack 7
Management 7
Functions 8
Operations 8
Transactions and Infrastructure 9
The GRC Lifecycle 9
Key Objectives of a GRC Architecture 10
Conclusion 11

Introduction to the RSA GRC Reference Architecture

Governance, Risk and Compliance (GRC) represents a business oriented approach to establishing ownership and accountability throughout the organization to improve decision making.

> **Governance** is the act of directing, controlling and evaluating the culture, policies, processes, laws, and institutions that define the structure by which organizations are directed and managed.
>
> **Risk** is the negative effect of uncertainty on achieving objectives; **Risk Management** is the coordinated activities to direct and control an organization to realize opportunities while managing negative events.
>
> **Compliance** is the act of adhering to, and demonstrating adherence to, external laws and regulations as well as organizational policies and procedures.

While these definitions may seem straightforward, establishing a GRC program within an organization is not a simple task. It is also not a new concept. Companies have been focused on improving compliance and managing risk for years. Since GRC programs have many moving parts, organizations are implementing an overarching vision of how things fit together to maximize value. This vision not only should clarify the objectives of a GRC program – but also give context to how the organization executes this strategic initiative.

The **RSA GRC Reference Architecture** provides a simple illustration to bring context to the discussion. It can serve as a backdrop as an organization plans out its strategy and delivers the core value message to the executives or simply as a method to start the dialogue. GRC is a complex topic and while no illustration will completely sum up the many facets of the effort, the GRC Reference Architecture provides a foundation upon which to drive the conversation.

GRC's Guiding Principles

Certain tenets should guide an organization's strategy for governance, risk and compliance. These guiding principles should be the foundation of the strategy and be part of the fabric of the GRC program. A GRC strategy is not a one-time effort; it is the establishment of a cultural shift in how an organization conducts business. The GRC program must define the elements necessary for governance, risk and compliance for an organization to meet its strategic objectives. A one-time effort will not meet that demand.

These principles must be ingrained into the GRC strategy:

- **Ownership.** The organization needs to hold individuals responsible for their actions and empower them to positively impact the organization. Management of risk and compliance issues cannot just be thrown over the transom. This includes not only establishing executive roles but clear responsibilities down to the front line employee.

- **Security and Peace of Mind.** At the end of the day, good governance, strong risk management and effective compliance efforts should bring positive assurance to the executives, shareholders, employees and applicable regulatory bodies. Risk and compliance efforts should focus on "what keeps people awake at night" as well as the many threats that could hinder the organization from achieving its objectives.

- **Sustainability.** GRC takes a persistent commitment to sustain the effort and achieve the strategic benefits. This has to be factored in when designing the program. For instance, while the effort to comply with an individual regulation may be at an acceptable level right now, the processes impacted by that regulation have a tendency to evolve and can quickly grow outside their original boundaries or intent. GRC must acknowledge this change and be considered a long term venture.

- **Consistency.** One can think of GRC as a big playbook the organization uses to manage risks and compliance issues. The GRC program involves many different processes – from overarching enterprise processes to daily operational processes. The GRC architecture should bring order to this large effort and get employees on the same page with a common framework and strategy.

- **Proficiency.** Once the business is executing using common frameworks and processes, the organization should then make sure that those efforts are as well-organized as possible as the organization becomes proficient in execution of risk and compliance management. GRC should invoke the concepts of continuous improvement and elimination of redundant efforts. Adjustments of processes to meet multiple goals can result in significant efficiency gains – generally more than initially estimated.

- **Balanced Effort and Reward.** The GRC program should be an effort with long term balance between the rewards of embarking on the journey and the costs associated with the journey. Organizations need to be smart and calculated in the way, level or extent that GRC activities are implemented. Organizations should be thoughtful about the cost vs. benefit of each incremental step in the execution of a GRC strategy.

- **Agility.** Given most organizations are in a constant state of motion, the GRC program must enable agile processes to react, respond and address changes to the business. Regulatory changes, new business opportunities, technology shifts and other factors will constantly barrage an organization and the risk and compliance implications must be managed in a manner that permits the business to adjust.

- **Transparency.** Finally, the concept of transparency should permeate the GRC program. Transparency means delivering the right information to the right stakeholders within timeframes necessary to enable proper governance. This transparency extends to both internal and external stakeholders and includes overall visibility into the structure of the program and the activities documented and managed within the program such as the status of strategies, business processes, risks, controls, and compliance with internal and external obligations. It is through the transparency of the GRC program that positive assurance of its effectiveness is demonstrated.

The bottom line for every organization is to make better and more consistent decisions across the enterprise that improves the likelihood that the organization will achieve its objectives. Along the way,

the organization becomes more certain that the activities managed within its GRC framework are aligned with the organization's objectives. This positive assurance of effective governance is reflected in a greater understanding of:

- where and how the organization is subject to risk,
- the amount of the risk accepted by the business,
- how risk-taking is aligned with the organization's risk appetite,
- how risk is not over or under controlled, and
- processes that exist to ensure that changes in risk profile are being adequately monitored and anticipated.

Along the way, the organization begins to find the equilibrium between risk taking and rewards; compliance spending and regulatory obligations; costs of security and the value of the assets and the other very important balancing acts challenging organizations today.

The RSA GRC Reference Architecture

The following illustration is the RSA GRC Reference Architecture:

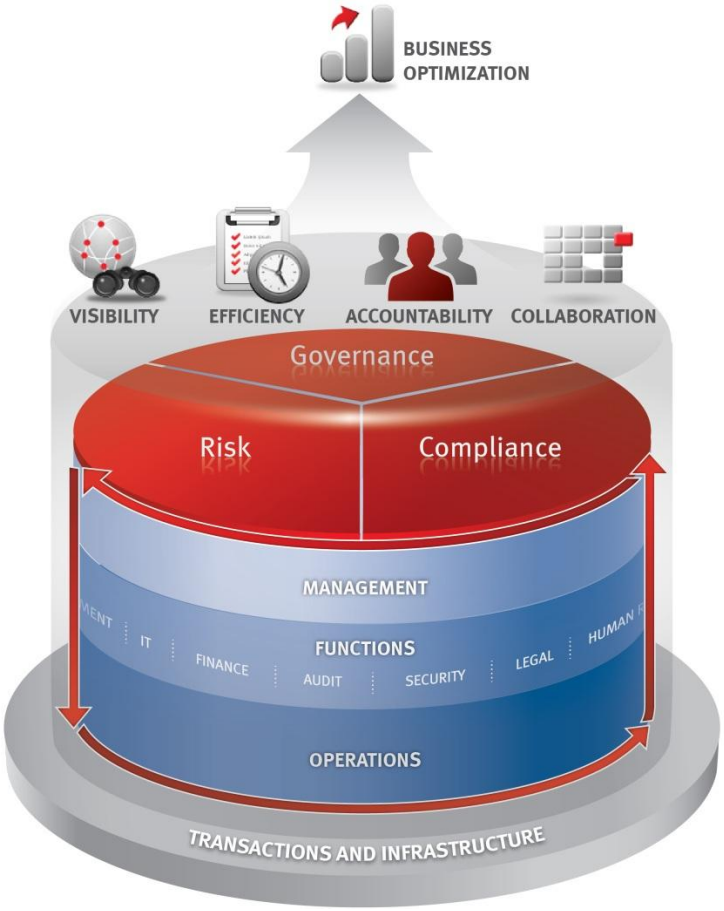

Figure 1: RSA GRC Reference Architecture

Business Optimization

Starting at the top of the illustration, the end goal of any GRC program is *Business Optimization.* GRC is a means to an end – not the end itself. Management and the Board of Directors are focused on making decisions that are more likely to result in desired outcomes for the organization. The GRC program should be part of the mechanism that empowers executives to keep this attention on the growth, constant improvement and optimization of the business. GRC programs should enable executives to understand risks to make the decisions that will mitigate, reduce or avoid risks or exploit opportunities to gain strategic advantages and drive the organization forward. The GRC effort of an organization should strive towards this final objective – optimizing the efforts of the business to bring stronger stakeholder return and value.

The Value Layer

The *Value Layer* depicts the outputs of the GRC program that lead to this Business Optimization. GRC programs deliver *Visibility*, *Efficiency*, *Accountability* and *Collaboration* through reporting, process enablement, ownership and collective, integrated strategies.

Visibility: The Board of Directors and executive management should be intimately involved in driving the overall vision for the GRC program. This vision should identify the necessary outputs needed to make the "big" decisions that ultimately drive the organization. The icon symbolizes the ability to connect the data together to see the overall picture and zoom in to track key risks or issues.

Efficiency: Through common processes, aligned goals and defined objectives, the organization should be marching together to optimize risk and compliance processes. The efficiencies should manifest in tangible (e.g. time savings/cost reductions) and intangible (e.g. anecdotal evidence) benefits of improved operations as illustrated by the icon.

Accountability: As the icon in the illustration denotes, the GRC program should make it evident who is stepping forward to own, manage, monitor and address risks and compliance issues. Establishing ownership and stewardship of risk and compliance is one of the most important values of the GRC program.

Collaboration: Collaboration is not just getting people to meetings to discuss the issues but also put the pieces together to see the big picture. The icon denotes that collectively, the organization can assemble a multi-faceted, organized view of risk and compliance, identify gaps and fill them in appropriately.

The GRC Core

Along the top of the "cylinder" in the illustration, represented by the red disc, are the core ***GRC Processes and Capabilities***. ***Core GRC Processes*** are the large, end-to-end, multi-faceted processes that facilitate the GRC program and enable the change within business operations needed to establish governance, manage risk and meet compliance obligations. For example, Policy Management – how policies are documented, rationalized and communicated – should be part of each domain and would be placed in the "Governance" layer of GRC. These Processes provide the frameworks and guidance across

the functions to build common approaches and consistency. The RSA GRC Reference Architecture uses the following as definitions for Core GRC Processes.

Governance

Policy Management – establishment of corporate policies, standards and supporting operating procedures based on business and regulatory requirements.

Enterprise Management – management of organizational assets, relationships and hierarchy.

Strategy Management – management of activities that connect strategic objectives to business plans and measures performance toward those objectives while factoring in risks and compliance obligations.

Risk

Enterprise Risk Management- establishment of a common risk management approach and framework to identify, catalog and monitor risks to the business.

Third Party Management – management of all external parties that support business operations.

Event Management – management of all situations (incidents, business disruptions, crises, etc.) that could adversely impact business operations.

Compliance

Compliance Management – management of activities related to measuring compliance of business operations to defined business practices and standards including adherence to external legal and regulatory obligations.

Audit Management – management of programs that provide an independent or objective measurement of the business operations and execution

The Organizational Stack

The cylinder within the Architecture depicts the multiple layers of structure and processes of the organization. One core understanding in GRC is that processes are not executed in a vacuum and may depend heavily on each other. For example, Risk Management cannot be discussed without some inclusion of controls based on corporate policy. Subsequently, the Compliance Management process should focus on those controls and thus inform the Risk Management process on the state of the controls. The *Organizational Stack* should be viewed as representing a continuum of people, strategies, methodologies and processes that work together for greater benefit.

Management

The Management layer represents the executive level of the organization and the overall driving strategy of the GRC program. Management in this context depicts the part of the organization that cuts across the company and represents the major work streams that are common across each function. Management – through common objectives, defined roles and responsibilities and shared technology enablers – guide business processes in the framework of the overall program goals.

Functions

The *Functions* layer represents the different business activities within the organization that will drive and benefit from a cohesive GRC strategy. Every organization may have different definitions of this layer as multiple parts of the business will play a role in the GRC program and the Functions included in the illustration are indicative of common segments of the business. The dotted lines in the illustration depict the fact that GRC is breaking down the silos that traditionally have remained separate or, at a minimum, are disconnected. For purposes of this document, three major functions will be used as examples:

- Information technology
- Finance
- Legal

The *Information Technology* function focuses on the business platforms and systems that support the overall technological infrastructure of the organization. Governance aspects of this domain include IT policies and procedures, roles and responsibilities for IT staff and the overall strategy to provide IT services. Key risks include data security, system reliability and capacity, disaster recovery and IT service delivery. Compliance aspects include the various data security regulations such as HIPAA or GLBA, support for financial systems for Sarbanes-Oxley (SOX) and the variety of individual industry requirements.

The *Finance* function focuses on the financial aspects of the organization including financial reporting and monitoring for impacts to the organization's bottom line. Governance aspects of this domain include financial reporting policies and procedures, accounting practices and roles and responsibilities for accounting and finance related employees. Key risks include any risk that can impact revenue and the financial standing or viability of the organization as well as financial reporting risks. Compliance aspects include adherence to accounting standards and financial reporting requirements including SOX.

The *Legal* function focuses on the adherence to the legal obligations of the organization as defined by laws, regulations and industry standards. Governance aspects include the structure of the legal counsel, regulations review and research and interaction between the business and external regulatory parties. Key risks include discovery acts or other litigation related activities, class action suits or any other action that could result in the organization being in "legal" hot water. Compliance activities are many as the legal domain is one of the key components to identify and interpret regulatory requirements for the organization and ensure proper practices are defined for the business operations.

Operations

The *Operations* layer represents the execution elements that assess and assign requirements to individual stakeholders, perform operational tasks, identify and respond to risk and compliance issues and promote an overall culture of accountability and code of acceptable conduct. As the bottom line in the chain of processes, activities within the processes will be guided by the Management and Functions.

Transactions and Infrastructure

Finally **Transactions and Infrastructure** cut across the bottom of the architecture and symbolize the daily operational events and technical fabric of the organization.

Transactions signifies the importance of the millions of individual events that could impact the state of the business. The organization must be mindful of all of the types of events that could impact the organization such as a change in a contract, a modification to a law, IT system and security events or even the establishment of a business relationship.

Infrastructure denotes the vast physical and technical foundation of the organization. Companies today depend so much on the technical infrastructure that any business process is going to have some touch point with technology.

These elements sit below the processes in the architecture since risk and compliance will be directly impacted by individual transactions or components of the infrastructure.

The GRC Lifecycle

The arrows within the cylinder denote the *GRC Lifecycle*. Outputs from Management level GRC processes, such as policies, controls and guidance, will drive functional and operational processes. Inputs into GRC processes from the day-to-day business (denoted in the Transactions and Infrastructure) will be collected, aggregated, summarized and "bubbled up" to provide information to management to support business decisions. The arrows depict on ongoing process that refines, improves and optimizes operations based on this flow of information. As GRC guides operational processes, data from operational processes informs "upwards" for management visibility. Based on that data, GRC processes should then help adjust and improve the operations.

For example, policies and control requirements will flow from a Core GRC processes such as Policy Management, and define management expectations for business operations. Then, compliance to that guidance, and the state of risk associated to the guidance at any given time will be dependent on many factors – many of them tied to operational processes, individual transactions and infrastructure – that will flow back into the GRC program. For example,

- The level of compliance to ethics obligations is dependent on actions taken by employees on a daily basis within operational processes.
- The level of compliance to financial regulations will be dependent on transactions processed via finance systems.
- The level of IT Security risk is dependent on the security events occurring on IT systems.

As Management sees the information flowing back "up the stack", the organization can then adjust the business to close gaps, better utilize resources, build efficiencies or improve effective operations. This constant flow of information drives the *Business Optimization* that is the overall goal of the program.

Key Objectives of a GRC Architecture

The GRC Reference Architecture depicts that there will be many moving parts to the overall program. Any effort that has so many critical objectives is bound to have multiple facets. This underscores the need for a strategic approach. Additionally, GRC is touching many parts of the organization. The web of stakeholders with varying requirements introduces a complex tug-of-war with opposing priorities. However, the scenario is not so grim. Significant redundancy in requirements, technologies and processes can be addressed by a common architecture and process approach to GRC. To manage the web of stakeholders, processes and objectives, we can use some common elements to guide our GRC strategy:

- **Unified.** The GRC architecture should strive to bring together related and common business activities into one cohesive approach. Most organizations have built governance processes within specific stovepipes in the organization. For instance, for SOX compliance, the financial organization has defined specific controls for financial reporting and the process is driven within the domain of Finance. With an enterprise approach, the organization can learn from this effort and apply control approaches across the organization to reduce risk and provide cross-discipline input into GRC efforts. The GRC program provides a structure for conversations to create a common language across the company for risk and compliance.

- **Automated.** Automation is critical to any GRC architecture. Due to the volume of data and information (represented by the Transactions and Infrastructure) involved in the risk and compliance processes, manual administration is impossible to contemplate. Automation will come in many forms – from correlating business data into consolidated views to automating risk and compliance management processes. Automation will also drive efficiencies and consistency throughout the program.

- **Information Integration.** A lot of time is wasted in connecting the dots across multiple risk and compliance efforts. For example, correlating manual controls during the financial reporting process with access control rules in the financial applications is a difficult task. The Enterprise GRC architectures should look to connect those dots in a meaningful way. In this example, understanding who can access financial data can add a new dimension to understanding manual procedural controls.

- **End to End.** Many times organizations will start or stop risk and compliance efforts mid-stream. For example, the organization may have identified security configurations for IT systems but fail to follow that through to look at the actual deployment strategies utilized within IT or the audit process used by internal audit to assess IT platforms. When an effort is initiated within an Enterprise GRC architecture, it has to be viewed from start to finish and the resulting approach has to be an end-to-end cycle that covers the risk or compliance requirement from inception to resolution.

- **Easy to Use.** GRC tasks are not generally the sole focus of the employee. Very few employees will or should have GRC in their job titles. An accounts payable clerk is just that – an accounts payable clerk – not a GRC accounts payable clerk. The Enterprise GRC architecture should account for the fact that controls must be inserted into the daily tasks of the employee in a way that allows him or her to get their job done without worrying about some GRC overhead or

having to check the GRC box. The Enterprise GRC architecture must talk to the employees in their own daily vernacular and make the tasks actionable and clear.

- **Flexible.** It does not take much imagination or experience to know that the core drivers of GRC involve many changes and transformations of business over time. The Enterprise GRC architecture must be adaptive in order to evolve as the business evolves. Furthermore, business users must be empowered to make changes without relying on costly, time-intensive re-engineering or re-development.

As an organization contemplates a comprehensive GRC Strategy – or even a portion of the GRC universe such as Enterprise Risk Management – these objectives should be embedded into the efforts. Core Processes, as depicted in the Reference Architecture, should complement and supplement each other and ultimately, come together into a cohesive strategy.

Conclusion

Governance, Risk and Compliance is an evolving field of focus for organizations today. In the past few years, it has grown in both criticality and value to organizations looking to deal with shifting business environments. The definition of GRC has matured in response to the changing regulatory and corporate governance needs. GRC initiatives can impact the entire the organization and has been a lightning rod to pull together functions within an organization that rarely collaborated in the past. The RSA GRC Reference Architecture provides a common illustration to discuss GRC strategies, articulate the many different levels and objectives of the initiative and give context for the high level vision.

CONTACT US

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

www.EMC.com/rsa