BUILDING A BUSINESS CASE FOR GOVERNANCE, RISK AND COMPLIANCE

FIXNIX

WHITEPAPER

CONTENTS

INTRODUCTION

The news headlines continue to report on fines imposed by regulators, a myriad of corporate bribery and fraud, and the challenges of driving business growth. This trend only serves to highlight that despite recent investment in compliance, internal audit, risk management, and corporate governance disciplines, significant assurance gaps exist in most corporations. While isolated incidents of one-time governance failures are bound to occur, long-term systemic failures are more than just an isolated anomaly.

Although fingers often point to one specific area of the company as the responsible party, these events are the result of much more than a couple of overlooked risk assessments or poor management judgments. They indicate that the assurance functions of legal, internal audit, risk management and compliance, in most cases, do not share business processes, terminology, technology, information, or a common assurance methodology. To address this shortcoming, the concept and discipline of end-to-end Governance, Risk and Compliance (GRC) has emerged.

Many organizations consider their legal, audit, risk management, compliance or corporate governance processes to be at an acceptable level of maturity. To assess where an organization is on the maturity curve, the question to ask is: *Could my company make the following representation to our shareholders or to the board?*

- We have a consistent process in place to understand current regulatory requirements and proactively assess of all of the regulatory changes that will impact the organization.
- We have identified the levels within our organization structure where accountability for GRC resides and have a common understanding of how GRC activities connect to the business processes that create value in our organization.
- The board and senior management have a common language to describe risks and controls, have visibility into all business risks, and a secure portal to share and communicate information.
- We have designed a standard, reliable methodology, developed suitable conceptual frameworks combined with information technology and assigned sufficient management accountability and resources across our organization to ensure our risk management information continuously meets our requirements.
- Our internal audit department evaluates the reliability of our risk management framework continuously and we adopt all necessary measures to ensure the reliability of our framework is maintained or enhanced.

Few, if any, companies could reliably prepare such a representation. At best, individual point-in-time silo-based reports on compliance, control or governance effectiveness might be available. But the concept of positive, continuous and verifiable enterprise-wide reporting does not exist in today's assurance world. To do so requires the implementation of an end-to-end approach to GRC.

ASSURANCE: THE LAST MAJOR BUSINESS FUNCTION TO BE INTEGRATED

The idea of end-to-end GRC—the connecting and strategically managing and reporting against the methodologies used by legal, compliance, risk, audit, and finance professionals, the information they produce, and their planning and reporting activities—is finding growing support. Integration of assurance function activities is being driven by boards who are insisting on better, more frequent and more granular reporting on risk, by regulators who are imposing more regulatory requirements, and by managers who are faced with hidden but increasing costs.

Driven by these business challenges, the term GRC has entered the professional lexicon. Over the past five years, many different definitions and variants of the acronym GRC have been published. There are probably as many definitions of GRC as there are companies that provide technology or professional services to address GRC challenges.

While every business needs to define what GRC means in their own organizational context, a great starting point to understand the broad scope and objectives of GRC is to use the definition provided by the Open Compliance and Ethics Group (OCEG). In its *GRC Capability Model, Red Book, 2.0* (April 2009), OCEG defines GRC as a "system of people, processes, and technology that enables an organization to:

- Understand and prioritize stakeholder expectations.
- Set business objectives that are congruent with values and risks.
- Achieve objectives while optimizing risk profile and protecting value.
- Operate within legal, contractual, internal, social, and ethical boundaries.
- Provide relevant, reliable, and timely information to appropriate stakeholders.
- Enable the measurement of the performance and effectiveness of the system."

The definition highlights that GRC is broad in scope and aspirational in outcome. GRC activities are by nature interconnected and rely on a common set of information, methodology, process and technology. By establishing a common, end-to-end discipline around research, documentation, monitoring and disclosure, organizations can replicate improvements in one GRC area across other GRC areas with the overall goal of uncovering business advantage and driving shareholder value. The result should be reliable achievement of business objectives while addressing uncertainty and acting with integrity.

CURRENT STATE OF GRC: THE CHALLENGES

GRC professionals are accustomed to change driven by professional standards or by regulators. Until recently, the vast majority of GRC projects were driven by external regulations or compliance requirements that offered little option over whether, when or how to implement. For example, the Sarbanes-Oxley Act and related PCAOB audit standards drove significant effort and influenced the methodology used to assess internal control over financial reporting. The business case for Sarbanes-Oxley compliance was simple: comply at any cost or face significant negative market impact or jail time for the CEO or CFO. The same can be said in regards to the mandated adoption of XBRL and many of the provisions of the Dodd-Frank act that are driving business change.

While response to these regulatory changes is necessary, the implementation of process change in isolation has resulted in an environment of working in silos, conflicting information and terminology, disparate technology, and a lack of connection to business strategy.

CHALLENGE 1: WORKING IN SILOS

In response to meeting the compliance requirements of a single regulation or driven by internal reporting structures and traditional functional roles; legal, internal audit, risk management, and compliance professionals often are found to work in very rigid silos, focused on a tactical set of departmental objectives. In this environment, too many white spaces exist where information is not exchanged and there is a lack of accountability among GRC groups. The obvious problem with this missing connection and functional overlap is inefficiency. A variety of GRC groups often duplicate efforts, wasting GRC resources and management time.

CHALLENGE 2: CONFLICTING INFORMATION AND TERMINOLOGY

With more than 12,500 regulatory changes made in 2010, keeping up with change and analysis on regulatory information is a challenge for most compliance officers. This challenge is amplified by the fact that most organizations do not dynamically link these changes and information to a standard set of policies, risks and controls. Historically, legal, audit, risk and compliance professionals have all operated using a different "language" of GRC and unique definitions for policies, risks and controls. The end result is the inability to effectively share information and the reporting of complex sets of redundant, overlapping information to the board.

CHALLENGE 3: DISPARATE TECHNOLOGY

GRC technology includes information solutions, documentation and workflow software, business and legal research, screening, and reporting and disclosure solutions. A natural outcome and a potential driver of a siloed approach to managing GRC business processes is using different technology solutions to manage each discrete assurance area. When a company uses disconnected solutions to manage risk management, internal audit, policy management, and compliance, it runs the risk of inconsistencies and inefficiencies that may lead to unnecessary high costs. Multiple systems with multiple deployments cause conflicting versions of the truth. A standardized suite of solutions resolves these problems and establishes a single source of truth for the entire enterprise.

CHALLENGE 4: NO CONNECTION TO BUSINESS STRATEGY

Since most GRC process change has been driven by a reaction to a specific regulatory requirement, most organizations have not mapped their GRC processes to business strategy. This challenge becomes significant when trying to justify an end-to-end GRC project. If the perception of the GRC professionals is that of cost center functions addressing tactical audit or compliance initiatives, a more comprehensive GRC project will be difficult to justify. To overcome this perception and gain the proper funding and support required, a business case that links end-to-end GRC needs to be developed.

BUILDING THE BUSINESS CASE FOR END-TO-END GRC

Initiatives for more sustainable compliance efforts and integrated GRC now experience a more complex approval process to receive organizational resources and funding. Many GRC professionals find themselves competing for funds with other departments and peer groups in their organizations. In order to successfully gain approval for a GRC initiative, assurance professionals need to build a business case that outlines the costs, benefits and process that will be used to implement the GRC initiative.

Building the business case for GRC would ideally begin with a sponsored and funded mandate from the board or senior management. However, in most cases, GRC professionals are faced with the challenge of educating the board, developing and communicating basic business value arguments, and committing to delivering higher level value over time including reduced business risk, greater control, and improved oversight in order to obtain funding for a GRC project. The balance of this whitepaper outlines some concepts to assist in building your business case.

CALCULATE THE CURRENT COSTS OF GRC

A starting point for any argument of cost reduction is to document and analyze your current costs. Since GRC has historically been managed in silos, very few organizations can quickly quantify their current GRC cost. There are three primary categories to consider: people costs, direct costs of supporting tools and technology, and the costs of GRC inefficiencies and failures. Setting a benchmark of your current GRC costs is critical in demonstrating the inefficiencies or your current environment and showing process improvement in your pursuit of end-to-end GRC.

People costs include the labor attributed to GRC processes from those that directly work in assurance roles and those that are contributors to GRC processes. Include the headcount and cost of activities of those working directly in internal audit, compliance, legal, and risk management functions as well as an allocation for the costs of the management team that supports them. Also, include the time and expense of business process owners spent testing controls, answering inquiries, and generating reports and disclosures.

For most organizations, the collection and analysis of the cost of labor will highlight many process and activity redundancies and areas for improvement. Since most assurance groups are understaffed as is, this exercise should not focus on staff reduction but rather on the redeployment of resources for more strategic activities that drive business value.

Technology costs include the cost of information subscriptions, software, hardware, implementation and maintenance and support. When quantifying these costs, make sure to include the many hidden costs of IT including the time allocated to IT staff to support GRC systems, outsourced IT labor costs, and consulting services required to keep your systems maintained. Since many organizations rely on multiple systems running on multiple platforms, there is usually a significant opportunity for cost savings by consolidating systems and/or pursuing an end-to-end enterprise GRC solution that is offered through a Software as a Service (SaaS) model.

Quantifying the costs associated with GRC inefficiencies, near misses and loss events is critical to the business case exercise. Calculating the costs of GRC inefficiencies is fairly straightforward and includes analyzing the cost drivers of external audit fees, process consultants, and the labor costs of redundant activities. The discipline of tracking loss events involves summarizing all dollar expenditures paid for:

- Regulatory fines
- Dollars lost due to business interruption
- Market cap losses related to impacts to brand or reputation
- Losses incurred due to poor management of business risk
- Losses attributed to fraud

Just as important to tracking loss events is the tracking of near misses. Near misses are typically quantified in issue tracking systems or as a discipline of risk management. If your organization does not currently track near misses, create an estimate by documenting potential events (e.g., FCPA fine from the Department of Justice), assign the significance of the event (dollar value), and a probability of that event happening (e.g., 20 percent). The value of your near misses is the sum of the expected value of all of the documented events.

BENEFITS OF END-TO-END GRC

Companies who are most successful at deriving the tangible benefits of end-to-end GRC start with a clear plan and set of objectives on how to drive this business value. As with all complex building projects, the building of a GRC initiative requires a detailed blueprint to define the scope, taxonomy, methodology and outcome of the project. In analyzing the benefits of GRC, the project should focus on five major points:

1. Defining the connected GRC lifecycle
2. Establishing a common language for risks and controls
3. Implementing consistent reliable methodology
4. Developing transparency, monitoring, reporting and disclosure
5. Leveraging technology

DEFINING THE CONNECTED GRC LIFECYCLE

Most organizations will typically point to increased efficiencies as the most immediate benefit of end-to-end GRC. The efficiency benefits are best quantified and gained by adopting a consistent lifecycle of GRC activities. The traditional siloed approach to GRC results in a fragmented approach that inevitably leads to inefficiencies, added costs and an inability to maintain compliance initiatives and make informed and accurate decisions.

GRC activities are by nature interconnected and rely on common information, methodology, processes and technology. By establishing a universal, connected approach to legal, compliance, risk, audit, and control processes, leading organizations have demonstrated that they can better leverage information, gain operational efficiency, and provide greater transparency into overall business risks. The connected disciplines of GRC can be represented in a four stage lifecycle:

- STAGE 1 is about identifying, researching, and understanding risks and regulations and evaluating their impact on business strategy. Effective GRC requires knowledge of all business risks, visibility into regulations and regulatory changes, and an understanding of the impact those regulations have on your firm.
- STAGE 2 is about developing, implementing and communicating policies and putting appropriate controls in place. In a connected GRC world, regulations are dynamically linked to policies, and policies are linked to risks and controls at the respective level of the organization and process structure.
- STAGE 3 involves managing processes, monitoring changes, tracking issues and loss events, screening clients and employees, and implementing appropriate remediation. This stage involves defining risks and associated controls, documenting tests and assessments, and arranging the appropriate audit trail to provide assurance.
- STAGE 4 addresses reporting and disclosures. Visibility and transparency of information between internal assurance groups is necessary for optimized GRC processes and informed choices by the board. Timely and reliable external disclosures drive business value by building confidence with regulators and shareholders.

ESTABLISHING A COMMON LANGUAGE

Connected GRC requires a common definition of the organizational context, processes, policies, risks and controls. When working in silos, individual GRC groups acting independently create the contexts they require. This leads to inconsistent definitions of core data, inconsistent ratings and inconsistent scoping, and may hide systemic problems, duplication and gaps in coverage.

To derive the benefits of GRC, all assurance groups must use the same organizational and process structures for planning their work, allocating resources and reporting. For most organizations, inefficiencies from assurance fragmentation are so great that huge savings are possible from taking the simple step of eliminating silos and operating on a common context of a shared GRC organizational and process structure. The outcome of these efforts will enable an organization to:

- Coordinate planning across all GRC functions
- Eliminate gaps and duplication in coverage
- Decrease time spent by business managers
- Increase ability to spot trends as they develop
- Utilize a single system of record for assurance information

The same argument can be made when looking at risk and controls. A comprehensive assessment of risks and controls requires the use of a standard risk and control taxonomy. Effective GRC requires that risks and controls be classified and reported against standard models on which GRC groups agree. For example, if malicious code is considered a risk type that is important to the organization, then all instances of malicious code risks should be categorized accordingly and reported as such wherever they occur. Organizations could decide which risks, defined by risk type, are critical to identify and manage across all contexts and by all GRC groups.

Without a standard naming convention or common methodology for determining or classifying risks and controls, assurance professionals from different disciplines are unable to share information. The cost of this siloed state, for many organizations, is a driving factor for GRC initiatives. Risk assessments are performed multiple times by multiple assurance groups on the same risks, and corporate boards are communicated a complex set of redundant, overlapping information.

On the contrary, the benefits of utilizing a common language for risks and controls are far reaching and include:

- Improved reporting throughout the organization
- Consistent coverage as all risks are considered
- Improved business performance as risks explain performance gaps
- Better decision making when decisions are risk-based
- Less external oversight and audits because controls are standardized

IMPLEMENTING A CONSISTENT, RELIABLE METHODOLOGY

Connected GRC requires a common methodology that guides what information must be captured and how it is gathered. Successful GRC projects define: which material regulations need to be tracked, what clients and vendors to screen, thresholds beyond which risks would require mitigation or additional management, definitions of what controls require testing, and rules governing the creation of issues for reporting and resolution. The intent of the common GRC methodology is to ensure all internal assurance groups address policies, risks, controls and associated GRC activities in the same way.

Examples of where agreement needs to happen between assurance groups include:

- Regulations that need to be tracked
- Top-down risk criteria that should be used
- Policies and processes that require risk identification
- Risks that must be assessed (type or level)
- Risk responses that require remediation
- Screening criteria and frequency
- Management of board reporting
- Disclosure processes and disciplines

By adopting a common and consistent methodology towards compliance, risk and control, organizations can benefit from:

- Aligned management and GRC assurance groups
- Reduced regulatory risk
- Improved external risk ratings – lower cost of capital
- Efficient resource allocation
- Increased management ownership
- Reduced conflict between assurance groups
- Increased management self assessment
- Reduced reliance on audits and inspections
- Earnings stability – no shock events

DEVELOPING TRANSPARENCY, MONITORING, REPORTING AND DISCLOSURE

Effective GRC dictates that management and staff have primary responsibility for assessing and reporting significant information on GRC objectives. More importantly, to assess the continued effectiveness of GRC efforts, all information on the status of risks and controls should be available for continuous reporting. If implemented effectively, connected GRC projects provide a common scoring and rating communication between management and the board of directors so that both have relevant information to fulfill their roles with respect to the GRC objectives.

Also, matters affecting the achievement of GRC objectives are communicated with internal and external parties who need the information, including boards and their committee members, shareholders, creditors, suppliers, customers, communities, governments and regulators.

The benefits of a consistent and disciplined reporting structure include:

- Availability of accurate and consistent reports
- Positive knowledge and reporting of risks and controls for all participants
- Integration of assurance functions through information
- Timely and accurate disclosures to regulators
- Higher share multiple – rewards for better governance

LEVERAGING TECHNOLOGY

The pursuit of connected GRC is only part technology or IT initiative. However, organizations on the leading edge of connected GRC rely on comprehensive information technology that addresses all GRC stakeholders. A natural outcome and a potential driver of a siloed approach to managing GRC business processes is using different technology solutions to manage each discrete assurance area.

When a company uses a wide array of solutions from different vendors to manage legal, risk management, audit, policy management, and compliance, it runs the risk of inconsistencies and inefficiencies that may lead to high costs. Multiple systems with multiple deployments cause conflicting versions of the truth. A standardized solution resolves these problems and establishes a single version of the truth for the entire enterprise.

GRC technology provides greater efficiency, improves collaboration, and reduces the time and resource costs associated with GRC processes. GRC technology enables organizations to break down the walls between legal, audit, risk and compliance groups and provides expanded value as organizations deploy the software across the enterprise. By unifying the many GRC process owners, a comprehensive software solution can eliminate information silos, redundant data entry and improve information transparency and communication.

The outcome of end-to-end GRC is that assurance professionals will leverage information and processes to form a unified framework that will result in:

- A shared repository of GRC information used for planning and reporting on the work of internal audit, risk management, compliance and other GRC professionals
- A common calibrated methodology allowing collaboration among GRC professionals and the ability for each group to rely on the work of others
- Accelerated strategic growth with clear visibility of business risk when entering into new markets, launching new products, or taking on joint ventures, mergers or acquisitions
- Increased business value and operational excellence through process automation, common methodologies and connected transactions across business functions
- Simplicity – clear, concise and easily accessible information that promotes sound decision making
- Increased transparency provided by executive dashboards and on-demand or automated reporting features
- A compelling business advantage to move faster than competitors, secure in the knowledge that you are working within regulatory requirements

CONCLUSION

GRC represents one of the most significant advances in the world of legal, audit, compliance, and risk management in many years. Unlike most changes in the field, it is being driven not by regulators and professional standard setters, but by leading edge practitioners, solution providers and service providers. The business case for end-to end GRC is compelling and is well within the grasp of most major corporations today. The frameworks exist, the methodologies are there and the technology problems have been solved. Best practices are quickly emerging and significant rewards with low investment and little risk await the pioneers.

About FixNix GRC Platform™

FixNix is the world's innovative, well awarded leading cloud GRC company.

The company combines industry expertise with innovative technology to deliver critical information for leading decision-makers in the financial, legal, tax and accounting, scientific and healthcare markets.

Our solutions dynamically connect business transactions, strategy, and operations to the ever changing regulatory environment, providing highly regulated firms with the knowledge to act.

Our client groups include compliance, audit, legal and risk functions within the organization. We partner with firms to manage their risk exposure and accelerate their business at every step.

The FixNix Cloud GRC Platform™ is suite of products provides powerful tools and information that enable proactive insights, dynamic connections, and informed outcomes that drive overall business performance.

FixNix Cloud GRC Platform™ is combination of the market-leading products like

- **FixNix Audit®,**
- **FixNix Risk®,**
- **FixNix Incident®,**
- **FixNix Compliance®,**
- **FixNix Asset®,**
- **FixNix Policy®,**
- **FixNix Controls®,**
- **FixNix Whistleblower®,**
- **FixNix Vendor®,**
- **FixNix Contract®,**
- **FixNix Fraud®,**
- **FixNix Financial Risk®,**
- **FixNix Global Trade Compliance®,**
- **FixNix Environmental Monitoring and Reporting®,**
- **FixNix Assurance®,**
- **FixNix Insurance Compliance®,**
- **FixNix Corporate Social Responsibility®,**
- **FixNix Environment, Health & Safety®,**
- **FixNix Board and Entity Management®,**
- **FixNix Brand & Reputation Management®,**
- **FixNix Business Continuity & Disaster Recovery® and**
- **FixNix Training & awareness®.**