

Prepared By:



Michael Rasmussen
Risk & Compliance
Lecturer, Writer, & Advisor

Foundations of GRC: Establishing an Enterprise View of Risk & Compliance

Burdened by Risk and Compliance Silos

Success in today's dynamic business environment requires the organization to integrate, build, and support business process with an enterprise view of risk and compliance. Without a new approach to risk and compliance, the scattered and non-integrated risk and compliance approaches of the past fail and introduce greater risk and regulatory threats to the business. A sustainable enterprise view of risk and compliance is one in which accountability is effectively managed and the business has a complete system of record – providing visibility to assess across a multiplicity of risk and compliance issues. This is supported today by technology that allows for the direct integration of controls within business systems to prevent and/or detect unwanted behavior. Business now requires that governance, risk, and compliance (GRC) controls be integrated into business processes, systems, and applications.

GRC solutions that operate autonomously from business processes introduce further risk in today's complex and distributed business environment. Organizations require an enterprise view of GRC that not only brings together silos of risk and compliance, but integrates them into the enterprise process and application fabric of the business.

Table of Contents

- Burdened by Risk and Compliance Silos 1
 - Isolated Risk & Compliance Silos Introduce Greater Risk* 3
 - Maturity Through Business Control & Performance Optimization* 4
- Delivering Value Through an Enterprise Architecture for GRC..... 4
 - Six Value Propositions of a Holistic Approach to GRC* 6
- Gaining an Enterprise Perspective of Risk & Compliance 6
 - Defining an Enterprise GRC Framework* 6
 - Architect Integrated GRC Systems & Processes* 7
- Successful GRC Integrates Into Business..... 8
 - Conclusion & Recommendations* 9
- About this paper 10
- About Corporate Integrity 11
- About Michael Rasmussen 11

www.Corp-Integrity.com
research@Corp-Integrity.com
+1.888.365.4560

Foundations of GRC: Establishing an Enterprise View of Risk & Compliance

Demands on corporate governance

As a result of increased pressure of risk and compliance oversight, the Board of Directors is rolling up their sleeves and becoming more involved as directors face greater personal risk and responsibilities within their roles. Beyond Sarbanes-Oxley, organizations are weary of increased regulatory actions, risk inherent in a highly competitive global environment, corporate litigation, demands of corporate social responsibility, as well as stakeholder/shareholder retaliation. The governance roles of the corporate secretary, board of directors, executives, and audit are responsible for making sure the organization is on course and meeting strategic plans and objectives while staying within defined boundaries of laws, regulations, values, and code of conduct. These roles are the aggregation point for a holistic view of GRC. They are concerned with the consolidation of corporate performance, compliance, and risk metrics that gets communicated to stakeholders and becomes a permanent record when entered into corporate financial statements and reports.

Multifaceted risk environment

Risk to the business is like the hydra in mythology - organizations combat risks to only find more and more risks springing into their awareness. Executives are battling to understand and manage enterprise risks. This is in response to complexity in business risks, reactions from legislators and regulators, and corporate rating agencies that have now turned their sites on evaluating corporate understanding, management, and response to enterprise risk. The result - Enterprise Risk Management (ERM) now has an impact on the viability of a business and the organization's corporate credit rating. This is forcing board and executive discussions on strategies for approaching ERM.

Another aspect driving risk management is the dynamic and global nature of business. As organizations expand operations, their risk profile grows exponentially. Organizations need to stay on top of their game by monitoring risk to their business internally (e.g., their internal controls and processes) and externally (e.g., the competitive, legal, and geographic environments) to stay competitive in today's market. Success in global business requires an organization to be keenly aware of global financial markets, economic directions, environmental issues, global supply chains, varying regulatory practices, and more.

Organizations are increasingly aware to the critical need to link enterprise risk management and corporate performance management. In order to manage corporate performance you also need to manage risk. For every key-performance indicator defined to meet strategic objectives there are corresponding key-risk indicators to monitor the uncertainty of hitting those objectives.

Growing regulatory environment

Organizations face an expanding regulatory environment with rapidly increasing requirements that burden business. Over the past thirty-plus years regulations have grown significantly as well as the penalties faced for non-compliance. Organizations face expanding regulations, increased fines & sanctions, and aggressive regulators and prosecutors around the world. Management has become all too familiar with terms such as deferred prosecutions, consent decrees, and corporate integrity agreements.

Compliance is not just about meeting requirements of external mandates - but also involves alignment and control to stay within voluntary boundaries of ethics, values, code of conduct, and the culture of risk taking and management. Reputation and brand protection is also a significant compliance and risk management issue in a global environment.

Trying to bring an enterprise view to compliance is difficult - as it permeates the organization. From employment/labor, quality, environmental, health and safety, security, privacy . . . the list of requirements and individual business roles managing compliance is legion. Overall, regulatory compliance is a key topic of discussion from the top of the organization down into the trenches of business operations.

A further challenge to compliance is a move toward principle-based regulation. The purpose of principle-based regulation is to move from checklists of requirements to a focus on outcomes. Organizations are not told how to comply but what they have to achieve. There may be multiple ways to achieve the outcome and the organization needs to chart its course to get

Foundations of GRC: Establishing an Enterprise View of Risk & Compliance

there. This requires integration of risk management practices with compliance – something that has not been done in many organizations to date.

Isolated Risk & Compliance Silos Introduce Greater Risk

With new risk and compliance issues constantly coming to bear, organizations need to tackle the problem at its roots. Instead of treating each risk and compliance issue as an individual problem (as they have in the past), organizations need to define a common process and technology architecture to manage risk and compliance across the range of issues faced.

The old paradigm of managing risk and compliance is a recipe for disaster. Organizations have been reactive as they used manual or point solutions for risk and compliance while being extremely fragmented in managing risk and compliance as individual efforts that do not relate to a broader risk and compliance. A reactive approach to risk and compliance leads to siloed initiatives that never see the big picture. The result is complexity, redundancy, and failure. The organization is not thinking how controls and processes can be architected to meet a range of risk and compliance needs – NOR do they gain an understanding on how risk management and compliance control impact corporate performance. An ad hoc approach to GRC results in poor visibility across the organization and its control environment, as there is no framework or architecture for managing risk and compliance as an integrated part of business.

A non-integrated approach to GRC impacts business performance and how it is managed and executed, resulting in . . .

- **Wasted resources and spending.** Silos of risk and compliance lead to wasted resources. Instead of thinking of the big picture and how resources can be leveraged to meet a range of risk and compliance needs, they are developed independently – and often end up being a band-aid and not integrated into business systems and processes. The organization ends up with varying processes, systems, controls, and technologies to meet individual risk and compliance requirements. This results in multiple initiatives to build independent risk and compliance systems – projects that take time and resources.
- **Poor visibility across the enterprise.** A reactive approach to risk and compliance combined with siloed initiatives results in an organization that never sees the big picture of risk. The organization ends up with islands of controls that are individually assessed and monitored - supported by scattered silos of technology that have not been integrated into the business itself. The business is burdened by multiple and differing risk and compliance processes and assessments. This results in poor visibility across the organization and its control environment, as there is no solution that integrates risk and compliance into business systems and processes across the enterprise.
- **Overwhelming complexity.** Complexity in multiple processes and approaches to risk and compliance is confusing to the line of business. Varying risk and compliance frameworks, manual processes, over reliance on spreadsheets, point solutions that lack an enterprise view introduce uncertainty and confusion to the business environment. Complexity increases inherent risk and results in controls that are not streamlined and managed consistently - introducing more points of control failure, compliance gaps, and unacceptable risk. Further, using technology that is not integrated into critical business applications to automate bad processes does not help the business (old complex process + new technology = expensive and burdensome old processes). Inconsistency in controls means inconsistency in documentation of risk compliance that can further confuse the organization, regulators, and business partners.
- **Lack of business agility.** A GRC strategy that does not integrate into business systems and processes leads to a reactive instead of a proactive approach. The result – a lack of agility that is caused by reactive approaches that are exacerbated by point technologies and siloed processes that are not at the “enterprise” level and lack analytical capabilities. When information is trapped in individual roles, spreadsheets, point solutions that do not integrate across the business – the organization becomes risk and compliance crippled. Technologies that are not truly enterprise in scope and lack analytical capabilities leave the organization struggling to gain a full perspective of risk and compliance that is needed when business changes. The organization is not agile to the dynamic business environment it operates in and becomes so wrapped up in spinning a multitude of risk and compliance plates that business performance is degraded. Business becomes bewildered in a maze of varying approaches and control requirements that fail to be addressed with any sense

Foundations of GRC: Establishing an Enterprise View of Risk & Compliance

of consistency or logic. And when GRC processes are not integrated into enterprise applications – it ends up being a band-aid that is more cumbersome on the business.

- **Greater exposure and vulnerability.** This is a further fruit of complexity – everyone is focused on their silo of risk or compliance. No one sees the big picture. No one is looking at controls holistically across the enterprise. The focus is on what is immediately before them and not what the business needs to protect itself in the long run. The business lacks the enterprise view it needs to preserve value and protect the organization. When risks and controls are managed in siloed groups – the enterprise lacks perspective to define a cohesive risk and control environment. One control can be mapped to multiple risk and compliance requirements instead of each control being managed independently. A one-to-one control to risk/requirement perspective brings greater exposure than a many-to-one control to risk perspective. This is exacerbated by many so called GRC solutions that focus on assessment and replacing spreadsheets, but do not align and integrate with business processes and enterprise applications. There is lack of unity and integrated risk and control management activities within business systems and processes. Additionally, varying and independent efforts of risk and compliance lead to a difficult process of demonstrating enforcement and audit compliance. All of this ends up in duplication, gaps, or crippled GRC activities and a business that is ill equipped for aligning GRC to corporate performance.

Maturity Through Business Control & Performance Optimization

What may seem like an insignificant risk in one part of the organization may very well have a different appearance when other risks are factored into its relationship and impact. Organizations face out-of-sync controls and corporate policies that are inadequate to manage risk and compliance. Organizations fail and are encumbered by unnecessary complexity because they manage requirements, risks, and controls within specific issues and do not look to see how a common integrated framework and architecture can bring efficiency to GRC processes. Further, executives are becoming aware of these redundant risk and compliance projects from different parts of the organizations wasting company time and resources with manual and laborious assessments that fail to leverage technology and information.

Modern business requires a new paradigm in tackling risk and compliance issues across the enterprise. No longer can organizations afford to focus on single risk and compliance issues as unrelated projects and assessment, nor can they allow software band-aids to masquerade as GRC that is not integrated into business systems. A targeted strategy addressing GRC requirements through common processes and integration into enterprise applications gets to the root of the problem. The risk and compliance complexity in today's business requires a common strategy and architecture to effectively manage GRC. GRC is a three-legged stool: governance, risk, and compliance oversight are each individual but interrelated necessary components for effectively managing and directing an organization. In summary - good governance is built upon diligent risk and compliance management processes.

GRC solutions that operate autonomously from business processes introduce further risk in today's complex and distributed business environment. Organizations require an enterprise view of GRC that not only brings together silos of risk and compliance, but integrates them into the enterprise process and application fabric of the business.

In today's business environment, ignoring an integrated view of GRC results in business processes, partners, employees, and systems that behave like leaves blowing in the wind. Organizations face a complex array of risk and compliance demands impacting business. The more extended and distributed the business - the more challenging risk and compliance is to manage. An integrated GRC architecture aligns them to be efficient and manageable. Inefficiencies, redundancy, errors, and potential risks can be identified, averted, or contained. This reduces risk exposure of the organization and enhances business agility and performance.

Delivering Value Through an Enterprise Architecture for GRC

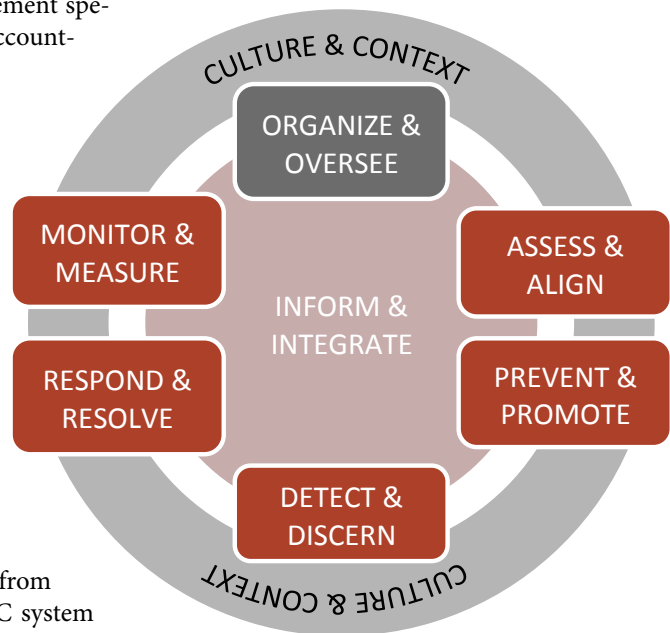
GRC is more than a catchy acronym used by technology providers and consultants to market their solutions. Ultimately GRC is about individual business roles within the organization working in harmony to create a collaborative environment for gov-

Foundations of GRC: Establishing an Enterprise View of Risk & Compliance

ernance, risk, and compliance. It is about collaboration and sharing of information, assessments, metrics, risks, investigations, and losses across these professional roles. It is about reducing uncertainty in business and producing predictable results. This unity of GRC is often handicapped when organizations deploy GRC technologies that are focused on assessments and audit functionality. The mature GRC environment is one that integrates control and oversight directly into business processes and enterprise applications.

The OCEG GRC Capability Model™ describes key elements of an effective GRC architecture that integrate the principles of corporate governance, risk management, compliance, ethics and internal control. It provides a comprehensive guide for anyone implementing and managing a GRC system or some aspect of that system. The OCEG GRC Capability Model™ is broken into eight components:

- **CULTURE & CONTEXT.** Understand the current culture and the internal and external business contexts in which the organization operates, so that the GRC system can address current realities – and identify opportunities to affect the context to be more congruent with desired organizational outcomes.
- **ORGANIZE & OVERSEE.** Organize and oversee the GRC system so that it is integrated with and when appropriate modifies, the existing operating model of the business and assign to management specific responsibility, decision-making authority, and accountability to achieve system goals.
- **ASSESS & ALIGN.** Asses risks and optimize the organizational risk profile with a portfolio of initiatives, tactics, and activities.
- **PREVENT & PROMOTE.** Promote and motivate desirable conduct, and prevent undesirable events and activities, using a mix of controls and incentives.
- **DETECT & DISCERN.** Detect actual and potential undesirable conduct, events, GRC system weaknesses, and stakeholder concerns using a broad network of information gathering and analysis techniques.
- **RESPOND & RESOLVE.** Respond to and recover from noncompliance and unethical conduct events, or GRC system failures, so that the organization resolves each immediate issue and prevent or resolve similar issues more effectively and efficiently in the future.
- **MONITOR & MEASURE.** Monitor, measure and modify the GRC system on a periodic and ongoing basis to ensure it contributes to business objectives while being effective, efficient and responsive to the changing environment.
- **INFORM & INTEGRATE.** Capture, document and manage GRC information so that it efficiently and accurately flows up, down and across the extended enterprise, and to external stakeholders.



An enterprise GRC architecture drives efficiency through avoiding redundant risk and compliance processes that bear down on the business and aligns risk management with corporate performance management. Resulting in what OCEG has called Principled Performance.

Foundations of GRC: Establishing an Enterprise View of Risk & Compliance

Six Value Propositions of a Holistic Approach to GRC

Organizations are approaching GRC to achieve an enterprise view of risk and compliance with a specific need to identify interrelationships in today's complex and distributed business environment. This requires that GRC initiatives involve a federation of professional roles – legal/compliance, risk, audit, IT, finance, and the line of business among others – working collaboratively to define common processes. This also involves the implementation of GRC technology that is integrated into critical business processes and applications and not separate from it. The goal is to achieve enterprise GRC . . .

1. **Accountability.** Organizations are in the hot seat – a multiplicity of risks, mandates, and requirements are attacking it from every angle. It is the organizations responsibility to manage GRC issues effectively, efficiently, and responsively. This requires a system of accountability where executives can see the status of GRC issues, events, incidents, and unresolved findings and hold individuals accountable for their resolution. The big picture of GRC is necessary with a drill-down into specific GRC areas. When issues arise – a lack of accountability and ownership of specific issues is a warning sign for regulators or investigators to dig deeper.
2. **Security – Peace of Mind.** In today's uncertain business environment plagued with global issues and threats the business wants peace of mind. Executives want to know that that 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 the organization to select and prioritize business controls aimed to bring systems and information in line within acceptable levels of risk tolerance.
3. **Sustainability.** Organizations demand a sustainable process and infrastructure for ongoing governance, risk, and compliance processes that are becoming more onerous. Further, organizations need to sustain their risk and compliance management practices on a continuous basis: as business is changing rapidly. Point in time assessments are no longer good enough by themselves. Business is changing hour-by-hour and minute-by-minute. The dynamic nature of business demands that an organization address GRC collaboratively and continuously.
4. **Consistency.** Organizations require that multiple roles in the organization start working together in an integrated framework and technology architecture. Business roles of governance, risk, and compliance need to understand how their roles fit into the big picture. Consistency has to be part of the technology environment where risks, requirements, and controls are defined and directly integrated into business processes and enterprise applications. GRC is getting everyone to play their different positions (roles within the enterprise) out of the same playbook.
5. **Efficiency.** The line-of-business is fighting back because redundant assessment and audit processes looking for similar information for different purposes is preventing the business from getting business done. This has a significant cost impact on the business – redundant and non-integrated GRC solutions have a harmful economic impact on the business. GRC, done correctly, aims to ease the burden on business by leveraging common processes, assessments, and information through technology integration and enablement.
6. **Transparency.** Business demands transparency across key-performance and risk indicators so it can monitor the organization's health, take advantage of opportunity, and avert or mitigate disaster. Corporate performance management is tightly related to risk management. When done correctly, performance and risk management are two sides of the same coin.

Gaining an Enterprise Perspective of Risk & Compliance

Defining an Enterprise GRC Framework

Responding to the corporate risk and compliance issues, organizations require a framework and technology architecture that integrates diverse systems and processes by providing a cohesive and common GRC process architecture.

Foundations of GRC: Establishing an Enterprise View of Risk & Compliance

Integration has become critical as GRC platforms need to tie into enterprise applications and infrastructure as well as play well with other GRC related applications.

Organizations are embracing technology to get away from document centric approaches to GRC that are based on paper, electronic documents, and spreadsheets. Organizations require a GRC architecture that can expand and contract to ever changing business initiatives over time. However, the first generation of GRC solutions have often been limited as they end up being a band-aid to replace spreadsheets and lack true integration into the enterprise application fabric and business processes. A primary consideration is the flexibility of the GRC architecture to enable the identification and resolution of business problems.

This paradigm shift away from rigid architecture that requires custom coding to change the solution or build out new solutions has become a thing of the past. No longer can businesses afford to deploy cumbersome GRC architectures that only a software developer can understand, maintain, use and update. GRC needs to be delivered as an integrated component of enterprise content, business process, and enterprise applications.

Architect Integrated GRC Systems & Processes

A properly defined GRC architecture is built upon common components that are adaptive to a dynamic business environment and integrated with critical enterprise applications. Risk and compliance burdens are not getting simpler – they are growing in number and complexity. No longer is risk and compliance about an annual audit; it now involves continuous monitoring in a dynamic ever-changing business environment. User identities are added, they change roles, and they are terminated. New business partner connections are established – others are torn down. IT infrastructures and applications are patched and configurations change. Sensitive information has become distributed and pervasive throughout the organization. Risk and compliance has to be sustainable as an ongoing and integrated part of business processes.

Continuously monitoring risk and compliance has become imperative but it's only cost effective if the organization has a strategic approach to managing controls across risk and compliance initiatives. The business is in an awkward position of reacting to mandates where it should be proactively managing controls and risk. The web of stakeholders with varying risk and compliance requirements appears to introduce a complex tug-of-war with opposing priorities. GRC requirements, risks, and controls have an impact on corporate strategy and performance and need to be monitored as part of an overall corporate performance strategy.

However, the scenario is not so gloom. There is significant redundancy in requirements, technologies, and processes across risk and compliance issues impacting the business that can be addressed by a common architecture and process approach to GRC.

Efficiency in risk and compliance processes is achieved through the definition of common processes and integration into the enterprise application environment that different stakeholders can utilize for their individual requirements as well as collaborate and share. A successful GRC strategy is one that has a symbiotic influence on the variety of business stakeholder roles and their common requirements.

Sustainable risk and compliance programs are built upon a common process and technology architecture designed to meet a range of requirements impacting the business. Organizations need to be intelligent about what processes and technologies they deploy – the goal is to define once and comply with many regulations, manage a range of risks, and maximize value from the convergence of technology, people and process. A sustainable approach to GRC results in an organization that is looking to the future and mitigating risk in the course of business as opposed to putting out fires by reacting to risk and control issues as they arise.

To achieve sustainability in processes organizations need to define a GRC architecture that is . . .

- **Unified.** All the stakeholders in risk and compliance need to be playing out of the same playbook. If different parts of the organization are going in different directions, risk and compliance will not be able to achieve the economies that a sustainable GRC architecture achieves. The goal is to provide sustainability and efficiency through a unified enterprise

Foundations of GRC: Establishing an Enterprise View of Risk & Compliance

view of the varying but related aspects of risk and compliance. An organization should be able to look through a single lens to see the complete view of risk and compliance as well as focus in on specific areas of interest.

- **Automated.** Business infrastructure is vast and rapidly changing. The only way to achieve effective GRC is to select and deploy technologies that help the organization automate risk and compliance processes and enforce controls within the environment. This requires GRC integration into enterprise applications. Through automation an organization achieves continuous risk and control monitoring as opposed to the point-in-time spot checks/assessments of the past.
- **Integrated.** A lot of time is wasted in deploying islands of technology that do not work together. Multiple points of management that span different areas of the infrastructure are costly to manage and do not provide a holistic view into the enterprise, and cannot correlate analysis to provide more definitive conclusions. Sustainable risk and compliance leverages an architecture that is integrated to facilitate management and reporting across the enterprise. GRC technology architecture is defined by common processes and being flexible to adapt to changing business requirements – it also has to be integrated with other systems and applications. Risk and compliance information is distributed and any core GRC technology needs the ability to integrate and work with other GRC technologies and information sources.
- **End-to-end.** The business environment is complex and distributed, which requires end-to-end management of risk and controls across enterprise assets, processes, identities, infrastructure, and information in the GRC architecture. This requires that risks, requirements, incidents, policies, and controls be managed across end-to-end business processes. When it gets down to it – knowledge is the center of risk and compliance initiatives and an organization needs an end-to-end strategy to define the accuracy and integrity of GRC information. GRC is ultimately all about the business process – vendors that do not offer an integrated enterprise view of GRC will handicap an organization.
- **Easy to use.** The users of GRC applications need to have the information and management of processes presented in a meaningful way that makes sense to the business. Business users need to find GRC processes easy to use and drive business efficiency. When GRC applications require a lot of technical interpretation it bogs down the process and frustrates the business.
- **Flexible.** A business GRC architecture has to be flexible. As stated, business is dynamic and GRC applications and information need to evolve as the business evolves. A flexible technology architecture is critical in making GRC adaptive and sustainable as business changes.

Organizations face an array of technologies to consider as the foundation of their GRC architecture. The challenge business professionals have is sorting through the maze of IT vendors all hocking their risk and compliance technologies.

To approach the maze of IT vendors, organizations should consider the range of risk and compliance requirements impacting the business and select a vendor that has the strongest enterprise GRC solution that is integrated into enterprise applications and focuses on business processes. The right technology architecture lays a strong foundation for a sustainable and effective GRC strategy.

Successful GRC Integrates Into Business

Risk and compliance management is complex with numerous individual intricacies and issues ready to frustrate the organization. Organizations that attempt to build a GRC strategy with home-grown solutions, spreadsheets -- or islands of technology that do not integrate into the enterprise and processes -- are left in the dark and boxed into a view of the world that they will find limiting down the road.

The case has been laid that the current business environment requires a new paradigm of GRC technology – a platform that spans across the organization and its individual risk and compliance issues, integrates into enterprise applications, becomes an integral part of business processes, brings together a GRC strategy ready to tackle risk and compliance issues at their roots, and is critically linked to corporate performance and strategy.

Foundations of GRC: Establishing an Enterprise View of Risk & Compliance

A successful approach to GRC requires:

- **Executive support/mandate.** GRC is a top-down issue that needed to be addressed and that the only way to adequately improve the organization is to get executive sponsorship for a managed GRC program.
- **Focus on preservation.** The current economic environment requires a GRC strategy focused on value preservation within the organization. Risk mitigation is currently critical in order to maintain continuity during turbulent times.
- **Alignment with corporate performance.** Identifying and managing new opportunities that a proactive and strategic approach to GRC provides the critical alignment of GRC to corporate performance and strategy – making GRC an integral part of ensuring that performance management is achieved.
- **Expediency.** The time to act was now – waiting only causes loss, additional issues and incidents to the detriment of the company.
- **Establish credibility.** There is synergy in understanding that gaining support from executives as well as middle management is critical to the success of GRC integration. Credibility is even more important during times of uncertainty.
- **Reduce redundancy.** The greatest value proposition was offered by reducing redundancy. This is strategically delivered through automation and alignment of a single set of foundation controls and delivered through automatic testing/validation of controls in the enterprise application and business process environment.
- **Integrate systems.** Long-term strategy should focus on integration of systems and developing a strong, sustainable and global technology architecture.

Conclusion & Recommendations

While comprehensive GRC is much broader than technology – GRC cannot be accomplished without technology. Technology is the foundation of GRC processes and provides the backbone of GRC communication and collaboration.

An organization's strategy for GRC success starts with a simple five-step plan.

1. **Identify the interrelated processes, problems, & issues.** An understanding of the scope of GRC issues, processes, technology, and requirements is the beginning. Organizations should start with a survey assessment aimed at identifying and cataloging the number of processes, technologies, methodologies, and frameworks used for risk and compliance across all business operations.
2. **Establish GRC program goals and objectives.** Once the organization has identified the scope of GRC across the organization it can establish the goals needed to achieve GRC. This starts with establishing a vision and mission statement for GRC that the goals stem from. Central to these goals will be a determination on GRC program structure – centralized, federated, or some form of deliberate but ad hoc collaboration. This structure will determine many other goals – particularly the consistent and relevant use of technology.
3. **Develop your short-term strategy for fulfilling GRC requirements.** With your goals in mind, identify the “quick wins” that will demonstrate GRC success and improvement. Aim for tackling the items that immediately show a return to the organization and build greater buy-in to the GRC strategy across business operations. This short-term plan should not be longer than 12 months.
4. **Conduct a comprehensive organizational risk assessment.** Part of the short-term plan should be a detailed risk assessment that provides a common framework and catalog of corporate risks across GRC management silos. This risk assessment is used to further identify and feed into the long-term comprehensive GRC strategy to help the organization better understand, manage, and monitor risk exposure.¹

¹ This assessment should be aligned with the OCEG Red Book Capability Model.

Foundations of GRC: Establishing an Enterprise View of Risk & Compliance

- 5. Provide a comprehensive action plan.** With the short-term plan in place – focused on the easy wins and process improvement – the organization can begin working on the long-term strategic plan that develops a comprehensive GRC strategy focused on process improvement. The harder and more challenging components of GRC should be brought into this plan. This plan is optimal when it covers a three-to-five year period.

Further advice . . . prioritization of risk and compliance activities needs to be decided at a business level so that IT clearly knows what to work on. This can be difficult as silos of risk and compliance can function buried within different functions of IT and the business. To overcome this and facilitate a top-down approach, a sustainable GRC strategy requires that the organization get executive buy-in and support. This provides endorsement of the effort and overcomes obstacles of silos wanting to work independently and do things their own way.

Getting started on a sustainable GRC strategy requires that the organization get a current assessment of where they are today, what is in place and already deployed, identify redundancies in technology, and find areas that might have been addressed but where the solutions are not scalable or manageable at an enterprise level. The gap analysis is aimed to not only identify the current state but to also help the organization prioritize their roadmap going forward.

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

About this paper . . .

This white paper is brought to you by SAP.

For more information, please visit <http://www.sap.com/sapbusinessobjects/grc>

About Corporate Integrity . . .

Corporate Integrity is a research advisory firm providing leadership in education, research, benchmarking, and analysis on the issues and corresponding solutions for corporate governance, enterprise risk, and compliance management.

Through ongoing research, interactions, and benchmark analytics, Corporate Integrity is the authority in understanding how organizations can foster a culture that “walks the talk” – where integrity is central to governance, risk and compliance (GRC) practices. Corporate Integrity educates organizations and GRC professionals on achieving sustainability, consistency, efficiency, accountability, and transparency in their corporate GRC practices.

In addition to helping organizations understand and improve their internal GRC processes, Corporate Integrity assists technology providers and professional service firms in aligning their sales, product, service, and marketing strategies to the requirements of the roles responsible for GRC.

With the deepest GRC expertise and understanding available in the market, Corporate Integrity has developed a range of service offerings to assist organizations, GRC professionals, technology vendors, and professional services firms focused on GRC.

About Michael Rasmussen . . .

Michael Rasmussen is the authority in understanding Governance, Risk, and Compliance (GRC). He is a sought-after keynote speaker, author, and collaborator on GRC issues around the world and is noted for being the first analyst to define and model the GRC market for technology and professional services.

With more than 15 years of experience, Michael’s objective is to assist organizations in defining GRC processes that are sustainable, consistent, efficient, transparent, and accountable. His thought leadership is tuned to:

- **Educate** GRC professionals within corporations to identify, understand, and analyze GRC strategies, drivers, trends, and best practices;
- **Assist** technology providers with alignment of their product and marketing strategies to the needs and requirements of GRC professionals; and
- **Collaborate** with professional services firms on their portfolio of GRC service offerings to better equip them to serve their respective clients.

A leader in understanding risk and compliance standards, frameworks, regulations, and legislation, Michael aims to improve corporate integrity through advancing GRC initiatives. He has served in leading roles in public policy contributions to US Congressional reports and committees, and currently serves on the Leadership Council and Steering Committee of the Open Compliance and Ethics Group. Michael has been quoted extensively in the press and is respected for his commentary on broadcast news channels.

In June 2007, Treasury & Risk recognized Michael as one of the 100 most influential people in finance with specific accolades noting his work in “Governance and Compliance: Saving the Planet and the Corporation.” Most recently, in October 2008, he was recognized as a “Rising Star in Rocky Times: Corporate America’s Outstanding Executives Under the Age of 40.”

During his career, Michael has worked in the market analyst, consulting, and enterprise sectors. Prior to founding Corporate Integrity, Michael was a Vice-President and top analyst at Forrester Research, Inc. Before Forrester, he led the risk consulting practice at a professional services firm in the Midwest. Earlier, his career included industry experience in healthcare as well as manufacturing.

Michael’s educational experience includes a Juris Doctorate as well as a Bachelor of Science in Business.