

Prepared By:



Michael Rasmussen
Risk & Compliance
Lecturer, Writer, & Advisor

Foundations of GRC: Enhancing Business Performance Through Risk Management

Establishing a Culture of Risk

Organizations are uninformed to the range of risk they face

While the market seems eager to grasp onto the phrase “risk intelligence,” it means nothing if corporations cannot take action on the intelligence it provides. Being intelligent is not the same as being wise – most organizations lack both risk intelligence and wisdom. There are organizations that acquire a lot of information, but without transforming this information into knowledge by

Mature risk management requires integrated business performance and strategy management. Risk management, if done correctly, is part of business strategy, performance, and objective management.

Table of Contents

Establishing a Culture of Risk	1
<i>Organizations are uninformed to the range of risk they face</i>	<i>1</i>
Defining risk.....	2
Articulating a corporate culture of risk management	3
Inevitability of Failure Through Siloed Approaches to Risk.....	3
<i>Not understanding enterprise risk management</i>	<i>3</i>
Individual business roles are overwhelmed	4
<i>Organizations lack multi-perspective, 360° risk awareness.....</i>	<i>4</i>
Integrating Risk Management into Performance Management.....	6
Effective risk management.....	6
Aligning risk with strategy and performance management	7
A Common Architecture for Risk and Performance Management	7
<i>The role of technology in integrated risk and performance.....</i>	<i>7</i>
Conclusion: Putting the Pieces of Risk Management Together	9
About this paper	10
About Corporate Integrity	11

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

Foundations of GRC: Enhancing Business Performance Through Risk Management

understanding the context of their business risks, they fail to make better business decisions. Risk is often completely disconnected from business strategy, objective, and performance management.

Organizations occupy a complex risk environment: They suffer from both internal and external risk. Geopolitical, financial and treasury, economic, operational, legal and regulatory environments compounds risk. Many organizations learn these risks often interrelate to create a much larger risk environment than each silo is independently aware of. When the organization approaches risk in scattered and isolate silos, there is no possibility to be intelligent, let alone wise, about risk decisions that could impact business strategy.

Additionally, organizations suffer from a confused approach to risk management. They lack insight and context into business, and fail to make a connection between risk management and performance.

While risk management is a pillar of governance, risk and compliance (GRC), it is often the most misunderstood, misapplied, and misinterpreted component. Risk professionals often have a myopic view of their work – a lack of imagination, foresight, or intellectual insight. They are comfortable with their quantification work and love Monte Carlo, Bayesian, and Value at Risk models. They do not always understand how risk interacts with governance and compliance to properly protect the organization, as well as keeping the organization on track to meet its corporate performance and strategy objectives.

Risk management is further handicapped by many organizational silos that fail to integrate and support business strategy and corporate performance. As Theodore Roosevelt said, **“Risk is like fire: If controlled it will help you; if uncontrolled it will rise up and destroy you.”**¹ Risk can help an organization or destroy it; it all depends on the organization’s culture, philosophy, and approach to risk management.

Business is about taking risk. Judge Mervyn King of the infamous King II Report on Corporate Governance said it well: **“Enterprise is the undertaking of risk for reward.”**² John Paul Jones, the first U.S. Naval hero in the Revolutionary War, said, **“It is a law of nature inflexible and inexorable that those who do not risk do not win.”**³ Organizations must take risk to make money – it is part of business. This is nothing new – it has been part of life, government and business since the dawn of time.

The questions organizations must ask:

- Does the business know its risk exposure at the business process level and operations level, as well as its aggregation to the enterprise level?
- How does the business know it is taking and managing risk effectively to achieve optimal operational performance and hit strategic objectives?
- Can the business accurately gauge the impact of risk-taking and loss on business strategy?
- Does the business have the information it needs to take timely action to alleviate risk exposure, and to seize opportunities while avoiding or mitigating negative events?
- Does the business monitor key risk indicators (KRIs) across key systems and processes?
- Is the business optimally measuring and modeling risk?

The bottom line: Risk is part of business – it is business. Organizations must understand whether or not they are taking the right risks, whether risk is being managed effectively, and how to monitor risk-taking. A cavalier and uncontrolled approach to risk is a result of a poorly-defined corporate culture around risk, and may lead to disaster. These practices will provide case studies for future generations about how poor risk management leads to the demise of corporations – even those with strong brands.

1 <http://riskczar.com/risk-quotes/>

2 http://findarticles.com/p/articles/mi_qa5377/is_200206/ai_n21315049/

3 http://thinkexist.com/quotation/it_seems_to_be_a_law_of_nature-inflexible_and/151491.html

Foundations of GRC: Enhancing Business Performance Through Risk Management

Defining risk

Clear definitions are necessary to lay a firm foundation to build upon risk processes. To properly understand and manage risk, organizations must work from common definitions.

Risk by the OCEG definition in Red Book 2⁴ is defined as . . .

“. . . the measure of the likelihood of something happening that will have an effect on achieving objectives; most importantly, but not exclusively, an adverse effect.”

Risk management is defined as . . .

“. . . the systematic application of processes and structures that enable an organization to identify, evaluate, analyze, optimize, monitor, improve, or transfer risk while communicating risk and risk decisions to stakeholders. The overriding goal of risk management is to realize potential opportunities while managing adverse effects of risk.”

ISO 31000 puts it in straightforward and simple, terms: Risk is **“the effect of uncertainty on objectives.”**⁵

Ultimately, “risk” and “risk management” have a variety of meanings across the organization. To build a consistent enterprise risk strategy it is necessary to work from a common definition of risk that all can agree upon – even though different parts of the organization may have their particular intricacies, frameworks, and risk tools.

Articulating a corporate culture of risk management

Risk management requires the proper context across the entire culture of an organization. The only way an organization can manage risk appropriately is if acceptable and unacceptable risk tolerances and appetites are defined and managed. The culture of risk tolerance at all levels helps formulate these tolerances: This is where risk management relies on governance. The board and management must clearly define and communicate the organization’s culture of confronting risk. If the governance function does not do this, risk strategy is left up to individuals and the integrity of the organization is in jeopardy.

Once a proper culture of risk management is defined it is established and communicated through policies and training. This is where risk needs compliance. Compliance is more than adhering to laws and regulations – it ensures the organization adheres to its risk culture, policies, procedures, and controls. In the case of risk management, compliance plays a critical role in communicating policies and validating that the organization stays within proper boundaries established by governance roles in the organization.

The elements of governance, risk, and compliance are the three legs of the GRC stool. Take one away and the stool becomes unstable.

A well-defined GRC environment not only does risk assessment and modeling, but also delivers definition, communication, and training on risk-taking and management. The system maps the interrelationship of risks to controls, policies, enterprise assets (such as business process, employees, relationships, physical assets, and logical assets), as well as incidents and loss to business strategy, objectives, and corporate performance.

Inevitability of Failure Through Siloed Approaches to Risk

Not understanding enterprise risk management

4 OCEG Red Book with its GRC Capability Model provides the only guidance that links governance, risk, and compliance together into a complete framework – delivering the GRC ‘Rosetta Stone.’ <http://www.oceg.org/view/RB2Project>

5 ISO 31000:2009 (http://www.iso.org/iso/catalogue_detail.htm?csnumber=43170) is the international standard being developed for risk management. It is based on the AS/NZS 4360: 2004 (<http://infostore.saiglobal.com/store/Details.aspx?docn=AS0733759041AT>) standard.

Foundations of GRC: Enhancing Business Performance Through Risk Management

For some organizations, enterprise risk management (ERM) is Sarbanes Oxley on steroids: it is nothing more than a deeper look into internal controls with some heat maps built on top. In this case, it truly does not provide an enterprise view of risk. In fact, many organizations are deceived by risk programs that focus on an internal view of risk, particularly in specific areas such as financial control. It also neglects other business, as well as external elements of risk a business faces across its operations.

Despite this misperception about how to approach ERM, organizations remain keenly interested. Some of this is driven from the emphasis that credit rating agencies such as Standard & Poor's put on risk management. Others seek solace in ERM to help drive through turbulent economic times. Many seek ERM to help manage uncertainty in a dynamic and distributed business environment that extends across complex global business relationships, where a small mishap may significantly impact operations and performance.

Individual business roles are overwhelmed

The challenge organizations face in truly managing ERM is the number of silos of risk management scattered across the organization. When these silos are focused on independent issues of risk, the goal of ERM is to tie all of these risk-management programs together to form a broader, transparent view.

Deloitte uncovered the impact of silos of risk on organizations in its Value Killers research.⁶ Deloitte studied the Global 1000 and found nearly half of these companies had a drop in value of 20% or more in less than a month (this was before the current financial crisis). In 80% of these cases (400 of the Global 1000) this failure originates from multiple risk factors, creating a greater risk environment when risks are managed autonomously in different parts of the organization.

Organizations continue to manage risk in silos, where distributed business units and processes maintain their own data, spreadsheets, analytics, modeling, frameworks, and assumptions. Operational risk platforms (if deployed) are typically not equipped to capture the complex interrelationship among operational risks that span global operations, business relationships, lines of business, and processes. Individual business areas focus on their own view of risk and not the aggregate picture of risk, failing to recognize substantial and preventable losses.

Organizations lack multi-perspective, 360° risk awareness

Another problem with risk management is that organizations lock into a static view of risk analysis and management. These organizations overly focus on heat maps generated from fairly static risk-assessment processes. The era of SOX and control self-assessments has propagated this further. Organizations end up with an ERM program that is nothing more than a slightly broader view of SOX, and financial controls with little perspective of true ERM.

To manage and assess risk – whether at the enterprise level or within specific business functions and processes – individuals must embrace new ideas. There will be “black swans”⁷ (the completely unexpected); however, there remain many risks that should never be a surprise, and are simply a failure in the organization to get a 360-degree perspective.

A simple two-dimensional view of risk (such as a heat map) can easily lull an organization into thinking they are managing risk well and can cause them to be caught off guard – particularly if the risk taxonomy and assessment process is static and does not provide for new inputs. Heat maps have their purpose, but alone are not enough. Consider:

- **The room around you.** If you take a picture of the room you get one perspective. If you take a thermal image you get another. If you take an X-ray you get still another perspective.
- **Going to the doctor because something is ailing you.** The doctor most likely will do a physical exam, might order some blood tests, and perhaps even do an MRI, X-ray, CAT scan or some other investigatory procedure.

⁶ http://www.deloitte.com/view/en_CH/ch/services/audit/riskperformancemanagement/article/c12c74168800e110VgnVCM100000ba42f00aRCRD.htm

⁷ Nassim Nicholas Taleb's book and research into how the unexpected impacts us. In *The Black Swan*, Taleb references the analogy that in Europe all swans were thought to be white until one day a black swan is discovered in Australia changing our perspective of swans. <http://www.fooledbyrandomness.com/>

Foundations of GRC: Enhancing Business Performance Through Risk Management

One software vendor markets a complete risk-management platform that is nothing more than a replacement for spreadsheets for risk questionnaires and assessments.⁸ Specifically, it offers no loss/event history. The vendor provides a beautiful heat map – but the information behind it is pure speculation from just a few subjective inputs from self-assessments.

The question is: *How does an organization begin to model risk and identify likelihood if it has no clue into the issues, events, incidents, losses, and investigations that influence any given risk area?*

To manage risk effectively requires multiple inputs and methods of modeling and analyzing risk. This requires information gathering – risk intelligence – so the organization has a full perspective of risk and makes wise decisions.

Effective risk management involves gathering multiple perspectives of risk information to enhance risk analysis. This includes gathering risk intelligence from:

- **External perspectives.** The organization must monitor the external environment for geopolitical, environmental, competitive, economic, regulatory and legal, and other risk intelligence sources.
- **Internal perspectives.** The organization must evaluate the internal environment of controls, audits, assessments, issues, events, incidents, corporate performance and risk indicators, and other internal data points.

Visualization of risk from multiple angles is critical. Good risk management involves taking external and internal perspectives and modeling risk in relational diagrams, decision trees, heat maps, scenarios, or even quantitative models involving Monte Carlo or value at risk simulations.

As organizations create enterprise, operational or other risk-management programs it is important to build a 360-degree multi-perspective risk analysis framework to allow it to think outside the box and look at risk from a variety of perspectives.

The challenge: Organizations must develop processes to harness internal and external information to be intelligent about its risk environments so it can make wise business decisions. This involves gathering information from the internal environment such as:

- **Losses.** What are the historical trends and patterns of loss to the organization?
- **Issues/events.** What events, issues, incidents, and investigations has the organization undergone?
- **Success and performance.** Where has the organization been surprisingly successful in seasoning opportunities and creating value?
- **Controls.** What is the state of controls in the environment? Are they effective?
- **Policies.** Does the organization have adequate policies and procedures? Are they current and up-to-date? Do responsible parties understand them?
- **Risk appetite.** Is the organization taking on too much risk or too little risk?
- **Risk management.** Is the risk taken adequately monitored and managed?
- **Compliance.** Are compliance obligations being met? Are there issues with law enforcement or regulators?
- **Culture.** Do employees understand and subscribe to the corporate ethics and code of conduct?
- **Business relationships.** Is there unwarranted risk, unacceptable values and ethics, or issues with compliance across third-party business relationships?

⁸ Spreadsheets are a recipe for disaster in risk management – they lack non-repudiation, integrity, an audit trail and provide nightmares of report consolidation and analytics when they are sent out to a wide array of users to gather risk information.

Foundations of GRC: Enhancing Business Performance Through Risk Management

Over the years, many organizations have matured in their view of internal risk intelligence issues. However, external environment issues remain disconnected to the risk information gathering process. External risks are managed in a variety of ad hoc ways with little accountability and oversight.

Risk intelligence of the external environment includes:

- **Legal monitoring.** Monitoring new case law, regulations, and pending legislation to predict the readiness of the organization to meet new requirements.
- **Geopolitical risks.** Monitoring countries that the organization has operations in or does business with to determine events that could have a positive or negative impact on the business. This includes civil unrest, terrorism, new laws, and business dealings.
- **Environment.** Monitoring environmental threats around natural or man-made events that could impact the organization, such as tornados, hurricanes, earthquakes, volcanoes, or disease.
- **Hostile threats and vulnerabilities/exposure.** Monitoring individuals, organizations, and governments that may be hostile to the organization, and looking for vulnerabilities and exposure to threats.
- **Financial risks.** Monitoring capital markets and conditions such as foreign exchange rates and commodities, so the organization can capture return and opportunity while mitigating and controlling loss. This allows for proper hedging.
- **Competitive environment.** Monitoring competitors to evaluate their strategies, products, services, marketing, sales, financial condition, and partnering performance.

Risk and regulatory-intelligent organizations must develop systems and processes aimed to intake risk information, model and measure its potential impact, weed through irrelevant information, and route critical information to specific individuals responsible for making a decision on the particular issue. This requires accountability management and integration with content and information aggregators in which the organization is profiled.

Integrating Risk Management into Performance Management

Effective risk management

Mature risk management requires integrated business performance and strategy management. Risk management, if done correctly, is part of business strategy, performance, and objective management.

Where risk is understood and evaluated as part of corporate strategy and performance, it is set in a business context and mapped to corresponding KPIs. The goal of a business strategy and performance-aligned risk management:

- Addresses opportunities, obstacles, and threats in a business context.
- Continually identifies obstacles and threats to business strategy and performance.
- Assesses the potential impact of threats to business strategy and performance.
- Identifies additional risks and related opportunities for further assessment.
- Assures risk-intelligent decisions by having risk information aligned with corporate objectives.
- Assigns risk ownership to the performance and objective area that it impacts.

Foundations of GRC: Enhancing Business Performance Through Risk Management

- Implements structures to enable the organization to appropriately pursue opportunities while addressing obstacles and threats that may hinder it.

Aligning risk with strategy and performance management

An effective risk-management program keeps corporate strategy and performance in view. This requires that the systems used to monitor corporate performance are integrated with the systems used to monitor risk. As organizations establish KPIs, KRIs should also be established for each performance area.

Risk management aligned to business strategy results in:

- **Risk aligned in the context of the business.** Risk does not operate as an island unto itself, but is defined and managed in the context of where the business is heading – its goals and objectives. Executives and management should clearly be able to see how risk supports or hinders execution of business strategy.
- **Risk managed within the context of business cycles.** An effective risk-management program aligns to the business and its strategic initiatives. Risk assessments, monitoring processes, and reporting must support corporate and board-level objectives, with appropriate business metrics.
- **Findings influence strategic planning and investments.** Risk management supports and enables the business to execute a strategic plan and optimize return on its investments.

Effective risk management not only supports business strategy but is also integrated into ongoing monitoring of corporate performance management. Most risk systems and technologies fail because they have no insight or integration into corporate performance management. Risk supports corporate performance as it enables:

- **Alignment** of resources to address critical risks that can hinder performance.
- **Management** of risk through improvement plans and monitoring set in a business context aimed to optimize return.
- **Better business decisions** driven by measurable metrics – KPIs are mapped to corresponding KRIs.
- **Business process and function efficiency**, making risk a part of business and not a bolted-on process with questionable value.

A Common Architecture for Risk and Performance Management

The role of technology in integrated risk and performance

Most vendors marketing risk-management platforms simply replace spreadsheets and do not deliver a full picture of enterprise risk. If the platform just provides surveys and assessments it does not truly do risk management. Buyers of risk technology should challenge risk vendors that come peddling their software: Ask how the application manages risk by providing integration across financial, treasury, market, credit, commodity, operational, and regulatory risks. Most vendors are stumped on this question alone. Explore how the solution delivers multiple modeling scenarios and risk analytics. Find out how the system integrates and becomes a seamless piece of the business performance and strategy systems.

Increased demand for risk management requires effective technology to support a comprehensive system of record to manage operational risk in a systematic way – across the entire business, including its business relationships and the external risk environment. Critical components of a risk-management platform are:

- **Risk-framework flexibility.** The goal of ERM is to provide harmony across a range of frameworks, standards, and approaches currently used across the enterprise. Different risk areas have unique needs and standards. The risk-manage-

Foundations of GRC: Enhancing Business Performance Through Risk Management

ment platform must be able to adapt to different risk categorization, taxonomies, measurement schemes, and evolve as risk processes mature over time. A robust ERM platform can harmonize and provide fluidity across these frameworks.

- **Risk intelligence.** These days every vendor has a dashboard to model and report on risk. However, they fall down when it comes to direct integration with business systems and applications across multiple ERP systems, instances, and proprietary enterprise applications. Further, most do not integrate with corporate performance management. This goes against what risk management is about. Risk management, done properly, is all about managing risk in light of corporate performance. For every KRI there should be corresponding corporate performance indicators, and solutions should provide the ability to manage KRIs in the context of KPIs.
- **Risk management breadth and depth.** Risk management is more than just managing the downside of risk; it is about optimizing risk-taking to seize hold of opportunity and return to the organization. Organizations stuck in managing the negative, which neglect the positive side of risk-taking, miss what ERM is about. A robust risk-management platform has sophisticated modeling capabilities that can demonstrate positive returns, not just the downside. This requires in-depth risk modeling and analytic capabilities to measure and model risk.
- **Risk visualization.** Nearly every vendor has latched onto heat maps as if they are the only way to visualize risk. Granted, heat maps can be useful – but they are not the end-all of risk visualization. Good risk management requires multiple visualization models. A risk manager must be able to look at risk from different views and angles to identify intricacies, relationships, and exposure. Different pictures tell different stories. The same is true with risk visualization – organizations need multiple ways to visualize risk to comprehend the full picture. A good risk system allows for modeling of loss, provides scenario analysis, and offers different ways to quantify and qualify risk while relating it back to corporate performance and objectives.
- **Risk process management.** Enterprise risk management requires flexible workflow and process management. Bringing together the many factions of risk management across the enterprise demands a platform that easily models business processes and workflow, and provides great flexibility and customization.
- **Risk integration - herding the silos of risk.** ERM is like herding cats – different parts of the organization have implemented their own risk solutions adapted to their specific needs. A good risk-management platform provides integration with specialty platforms that manage specific areas of risk.
- **Risk and control assessment.** This includes risk identification, assessment, surveying, and analysis. To manage operational risk, an organization will implement a taxonomy of risks and a framework designed to provide a sound and well-controlled operational environment. In addition, organizations must manage the balance between the cost of controls and the reduction in risk that the controls effect. The platform should support a range of assessment styles, including qualitative and quantitative assessments, as well as top-down and bottom-up techniques. Risk measurement should cover both inherent and residual risk metrics.
- **Internal loss events.** Operational losses are increasing in frequency and impact because business has grown more complex, particularly as transaction volumes increase, organizations use distributed operations, as business relationships grow, and as reliance on automated systems outpace the ability to monitor risk. Critical requirements for a risk-management process include capturing loss information. This includes creating a consistent categorization scheme for loss events (such as Basel II causal categories for losses), and linking loss to the risk taxonomy. This is extremely important since it allows an organization to pinpoint the root cause of losses and determine if certain controls are failing. This process facilitates continual optimization of risk management as well as the control environment. An operational risk-management (ORM) platform needs to combine assessment data with loss-event data to support an ORM process.
- **External loss data.** External losses are also a key component of a risk-management platform. The solution should support automatic upload and download capability for interfacing with external loss consortiums or commercial providers. In addition, the system should facilitate use of external loss for capital modeling, scenario analysis and benchmarking.

Foundations of GRC: Enhancing Business Performance Through Risk Management

- **Key risk indicators.** Continual monitoring and management of KRIs - including trending and aggregation- is a critical element of a risk-management process. A risk-management platform supports automatic notification to risk owners when KRI values reach thresholds. Workflows should automate ORM process such as KRI review and analysis. KRIs must support thresholds and time trending. The best systems also allow alignment of enterprise performance management with risk management, and provide a view into risk optimization as opposed to simply risk mitigation. Organizations take risk, and need assurance they are taking the right risk to meet objectives and that risk is effectively monitored and managed.
- **Reporting.** A risk-management platform must provide timely and accurate information to risk managers, risk owners in lines of business, senior and executive management, boards, and external constituencies such as auditors and regulators. Risk-management reports enable management to maintain risk at appropriate levels within lines of business, escalate issues and provide consistent data aggregation across business roles and functions. With improved visibility into its risk environment, an organization is in a position to make risk-intelligent business decisions. The risk-management platform must support a variety of risk reports including high-level dashboards, risk models, and detailed reports. It has to be able to aggregate data across business entities, relationships, risk categories, event types, and time periods.
- **Extensible and flexible platform.** One-size-fits-all does not apply to ERM. Organizations need an adaptable solution and process to meet specific needs, taking into account corporate governance including corporate policies and procedures. When choosing a technology platform, organizations must choose an application that can adjust to its process instead of adjusting the organization's processes to fit the application. Important areas for extensibility include:
 - **Business hierarchy.** Multiple hierarchies (legal, finance, organizational), multiple levels (with no limit), and asymmetrical hierarchies are all essential to conform risk management to the business.
 - **Localization.** As most firms operate in a number of localities around the world, many of which have their own local reporting needs, it is essential that the technology solution can be deployed enterprise-wide and can be effective across all geographies and business functions.

Conclusion: Putting the Pieces of Risk Management Together

A mature risk-management program does not operate in isolation from the business. A mature risk-management program is integrated with corporate performance, strategy, and objective management. This requires that the organization relate performance to risk, allows for multiple inputs impacting the risk environment from both internal and external contexts, and has a variety of ways to look at risk information to analyze, model, and relate risk back to performance and strategy.

Effective and mature risk management delivers:

- **Alignment of risk in the context of business strategy.** Risk strategy is fully integrated with business strategy where business management realizes risk management is an integral part of business responsibilities.
- **Risk intelligent business decision-making.** Risk-management culture and policies are effectively applied across the organization, supported by management. The business has what they need to make risk-intelligent business decisions.
- **Risk-based business planning.** Risk is a key component in business planning. Risk assessments and reports are structured to complement the lifecycle of the business to help executives and the board make effective decisions.
- **Establishment of risk culture and policy.** Risk policy is clearly communicated across the business and is effective at establishing a culture of risk management. Risk policies are current, reviewed and audited on a regular basis.
- **A risk appetite harmonized with business strategy.** Risk appetite and tolerance levels are established and reviewed. They are mapped over to business performance and objectives.

Foundations of GRC: Enhancing Business Performance Through Risk Management

- **Integration of risk and performance monitoring and metrics.** Defined KRIs are in place and appropriate mapped to business KPIs. Risk indicators have established limits/thresholds, and are defined at all levels of the business, its operations, and relationships.
- **Communication of business relevant risk information.** Risk reporting and indicators are relevant to the business and effectively communicated. Risk information adheres to information quality, integrity, relevance, and timeliness to the business.
- **Ownership of risk within the business.** Every risk, both at the enterprise as well as business process level, has clearly established risk owners. These owners represent roles that can take action on the risk.
- **Holistic awareness of the range of risks the organization faces.** The organization has defined risk taxonomy at the enterprise level which drills down into specific risk areas. A regular process is in place for risk identification to keep the taxonomy current. Various risk frameworks used across the enterprise are harmonized into an enterprise risk framework.
- **Multi-perspective risk analysis.** The organization uses a range of risk correlation, stress testing, and scenario analysis. Various qualitative and quantitative risk analysis techniques are in place and the organization has an understanding of its historical loss to feed into analysis.
- **Effective risk treatment in context of business objectives and strategy.** Risk treatment plans – whether acceptance, avoidance, mitigation, or transfer – are in place and monitored for progress. Audit functions conduct regular reviews. The solution reviews risk-treatment plans.
- **Governance of risk from the board down into the business.** The organization has a role and system in place to aggregate risk information across the business and effectively communicate, monitor, and manage risk. There is effective communication and accountability for risk oversight at the board of director's level.
- **Visibility of risk as it relates to performance and strategy across the business.** An enterprise view of risk is in place and maps over to corporate performance and strategy. Risk is effectively communicated to stakeholders and the organizations track record shows successful taking and management of risk.
- **Consistent ranking and measurement of risk.** Risk is categorized and structured according to its impact on business strategy, performance, and optimization.

Successful organizations face the challenge to move from immature to mature approaches to risk management. Immature risk-management programs operate in silos and are disconnected from each other: no consistency or efficiency is gained. Many ERM programs are not much better than this, as they are nothing more than an enhanced SOX strategy, focusing on a slightly expanded view of financial and other internal controls. A mature risk-management program is a seamless part of business performance, strategy, and objective management. Risk must be managed within the context of business. This requires the organization to take a top-down view of risk led by the executives and board, and make it part of the fabric of business, not an unattached layer of oversight.

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.