Risk Management: Protect and Maximize Stakeholder Value

An Oracle Governance, Risk, and Compliance White Paper
February 2009

ORACLE

I. WHY RISK MANAGEMENT?

"Risk Management is a key business process within both the private and public sectors around the world. Effective risk management and the resulting controlled environment are central to sound corporate governance and for this reason, much of the law that has been created in response to corporate collapses and scandals, now requires effective risk management."

International Organization for Standardization (ISO), April 2008

If the financial crisis has taught us anything, it's that this failure of oversight and accountability doesn't just harm the individuals involved, it has the potential to devastate our entire economy.

—Barack Obama, December 2008, in appointing the new Chairman of the Securities and Exchange Commission

Business survival requires organizations to take risk. Successful firms manage risk well while those that do not suffer. The unprecedented breakdown of credit markets and eye-opening demise of well established financial institutions have led companies small and large to pause, look at themselves, and ask: What's *our* risk? Do we have a handle on it? Is that good enough?

Recent actions from regulatory bodies and ratings agencies have also highlighted the need for risk management. For example, the Public Company Accounting Oversight Board (PCAOB) is guiding audit firms to pay more attention to the level of risk associated with management processes. Assuming management is likely to accept greater risk when acting under economic pressure, the PCAOB is encouraging auditors to adjust their audit plans and increase monitoring for high risk behavior.

Meanwhile, Standards & Poor's (S&P) is taking a closer look at risk management practices. Since 2005, S&P has included risk management analysis in its rating evaluations of financial, insurance, energy and agribusiness companies. Such analysis was easy to apply to those sectors because standard risks (e.g., market risk, credit risk, underwriting risk, trading risk) lent themselves to quantitative measures and hedging strategies. Building on this experience, S&P is now expanding its risk management and credit worthiness evaluation to all other companies. With the intent of developing benchmarks and implementing a scoring system to fine-tune companies' overall credit ratings, S&P analysts are having risk management discussions in their regular company credit reviews, with an emphasis on risk culture and strategic risk management.

Performance and risk are inextricably linked. An "Investors on Risk" poll run by Ernst and Young back in 2005 showed that sixty-one percent of investors would walk away from an investment if they thought risk was not adequately identified. To this day, however, many companies continue to ignore or misunderstand the opportunities that are derived from proper risk management. By establishing a consistent and disciplined process for managing enterprise risk, organizations can improve the predictability of their business results and reduce share price volatility. Better managed risk earns companies better ratings, allowing them to take advantage of lower costs of capital.

The question then is: what has held organizations back from a broader adoption of risk management programs?

II. RISK MANAGEMENT IN PRACTICE: STILL IMMATURE?

"Risk management as a discipline in business has been around for a while, but the collapse of credit markets would suggest it's still in its infancy."

Richard Phillips, Risk Management Professor at Georgia State University, December 2008

More than 65 percent of CFOs and more than 70 percent of audit committee members say managing enterprise risk is the biggest challenge their organizations face in the coming 12 months. The results suggest Enterprise Risk Management (ERM) is a challenge even greater than financial reporting and improving internal controls.

—The Changing Landscape of Risk Management, CFO Research & Crowe Group, August 2008

From the global financial crisis to the ensuing market volatility, decline in consumer confidence, and extreme fluctuations in energy prices, recent events have demonstrated that uncertainty is all around us. Despite companies' acknowledgement of the factor called "risk", uncertainty and risk have not been formally managed. Only fifty-two percent of chief financial officers surveyed by IBM in a 2008 CFO Study confirm having any prescribed risk management program. A mere twenty-nine percent align risk with performance by creating risk-adjusted forecasts and plans. Unsurprisingly, less than twenty-five percent of companies view their performance as "excellent" on any specific risk management tasks, according to Crowe's 2008 Risk Consulting Practice survey. Evidently, there is room for improvement. Several factors have contributed to the relative immaturity of risk management in most organizations.

A. Lack of Executive Commitment to Risk Management

While the involvement of senior management is arguably critical to the success of any initiative, it is absolutely essential for risk management. The reason is simple – certain aspects of risk management run counter to human nature. While people are eager to talk about favorable results and success, they are generally less enthusiastic when it comes to discussing actual or potential losses that affect their business. Without a demonstrated commitment to the risk management process from the highest echelons of the organization, a culture for success and managerial invincibility will prevail where past achievements provide protection from future risks and good management is enough to prevent troubles from arising. Problems are considered managerial failures to which risk management draws unwanted attention.

B. Fragmented Risk Management Activities

Most organizations will tell you "we already do risk management". While this may be true, many operate in silos with narrowly focused, functionally driven, and disjointed risk management activities. Systems are patched together. Human and information resources are duplicated. With so many disconnects, the company cannot achieve a timely and enterprise-wide view of risk. It is left in a state of risk ignorance where interdependent risks are not anticipated, controlled or managed. Threat to the business is exacerbated by aggregate risk exposure. In contrast, in a risk-intelligent company with a proactive and comprehensive approach, the management of risks supports every project across every function. Risk management becomes an integral aspect of organizational life.

Between 2004 - 2007, 62% of global companies experienced risk events that were primarily non-financial. Almost half were not prepared.

— IBM Global CFO Study, 2008

C. Risk Management is Historical; Not Predictive

Would you agree that things rarely turn out as expected? Until now, organizations have mostly concerned themselves with a historical and static approach to risk. Evaluating risks and identifying the critical factors to manage the range of potential future outcomes is often overlooked. With scenario-based planning however, risk management can yield insights on emerging dangers and make upfront mitigation strategies possible. For this to become a reality, organizations need the capacity and intelligent monitors in place to foresee unacceptable levels of risk and prepare for what might be.

D. Lack of Alignment among Corporate Strategy, Strategic Planning, and Risk Management

When a company attains the highest level of maturity, it typically requires that dedicated resources for risk management be integrated into business processes through a formalized procedure. In such environments, proactive risk management is systematically incorporated into corporate strategy and strategic planning activities. However, many organizations have grown an internal maze of assessments as individual responses to various risks while omitting or misaligning the strategic risk. In a 2008 Enterprise Risk Management Practices survey from Treasury and Risk magazine, only thirty-two percent of CFOs and risk managers were very confident that strategic/business risk was adequately identified, assessed and managed. This compared to sixty-three percent of respondents feeling very confident on their management of financial risk and fifty-two percent on compliance or operational risk. Risk management must stay close to the business and the business must understand what the risk management organization is tackling. When corporate strategy, strategic planning and risk management come together, a more well-defined and direct path to achieving business value and objectives is assured.

III. KEY CONSIDERATIONS FOR IMPLEMENTING A RISK MANAGEMENT PROGRAM

While a company may die a quick death if it fails to manage its critical risks, it will certainly die a slow death if it does not take on enough risk. Enterprise Risk Management (ERM) models -such as COSO's 2004 Enterprise Risk Management-Integrated Framework, the 2006 Risk Maturity Model for ERM established by the Risk and Insurance Management Society and the 2009 ISO 31000 Standard on Principles and Guidelines on Risk Management Implementation- describe an approach for identifying, analyzing, responding to, and monitoring risks and opportunities. They can be the starting point to classify and manage mutually dependent risks and instill a common risk language within the enterprise.

A. Set Goals for Risk Management

By addressing all risks comprehensively as opposed to dealing with individual types of risks (such as IT risks, financial reporting risks, environmental or legal risks), risk management can quickly feel overwhelming. Objective setting is therefore key. There are three common goals for risk management, which also correspond to the stages that organizations typically go through in developing their risk management capabilities:

- Goal 1: Protect against downside risks
- Goal 2: Manage volatility around business and financial results
- Goal 3: Optimize risk and return

The combination of all three comprises Enterprise Risk Management, but each organization must decide which focus to take. When a company fails to clarify how it understands risk and what it wants to achieve with risk management, sponsorship and ownership for risk management may be deficient, risk appetite unqualified, risk prioritization flawed, and resources misallocated.

B. Define Risk Tolerance

Until now, many companies have neglected to set and communicate their risk appetite. At an acceptable level, risk is perfectly fine but it is imperative that management defines what that acceptable level is in the interest of achieving the company's goals. The danger surfaces when one person's definition of a high risk equates to another person's medium risk. The difference in perception leads to inadequate risk assessment results with underrated risks being ignored and overrated risks consuming excessive resources. Unfortunately, many organizations still have disjointed, periodic or inadequate assessments. It's no surprise that eighty percent of companies do not believe they are getting as much value from their risk assessments as they should. Only one in three says they achieve effective results that properly align activities with objectives in light of risk tolerance, according to the 2007 Open Compliance and Ethic's Group Risk Study.

SOX as an ERM Framework?

Can existing work on Sarbanes-Oxley (SOX) be leveraged to jumpstart an Enterprise Risk Management (ERM) program?

- **SOX dwells on assessing financial reporting risks while ERM delves into all types of risks, financial and non financial, internal and external**
- **Risk assessment can be an annual process under Sarbanes-Oxley while ERM is a constant process since organizations change and new risks emerge**
- **But some SOX best practices are relevant to ERM:**
  - **Reapply SOX risk assessment process to areas of risk management. Risk assessment may be limited in scope under SOX but the approach can be reused for ERM**
  - **Get commitment at the board and management level, leveraging the understanding they have of the value of reducing fraud risk, enhancing governance, and strengthening controls for effective ERM**
  - **Establish a risk department and appoint a chief risk officer or other key person to be responsible for the SOX or ERM process**

—ERM vs. Risk Assessment: An Analysis, Compliance Week, March 2008

C. Assess Risks Continuously

Considering an organization's risk appetite, assessments are crucial to monitoring risk exposure, treating unwanted risks and seizing emerging opportunities. In fact, attaining a unified and continuous approach to risk assessments has direct impact on business plans with:

- more targeted internal audit plans
- greater operational visibility and performance
- better decision making
- improved strategy execution

It is also critical to conduct risk assessments in a disciplined fashion. Without a standard risk taxonomy and common methodology for evaluating risk severity and probability, risk assessments can become a bureaucratic exercise that yields few benefits and worse, results in ill-informed decisions.

D. Report Risk Information

Still, deriving value through risk assessments can only be possible with the appropriate reporting mechanisms. When critical risks are properly flagged, the organization can respond, if not anticipate, risk with timely insight into its cause, impact and options for resolution. Thanks to a complete view of enterprise risk, important risk factors become apparent to executives and boards of directors and can be swiftly incorporated to strategic and operational planning.

IV. ORACLE'S COMPREHENSIVE PLATFORM FOR RISK MANAGEMENT

"Risk processes should be carried out in the context of where a business is headed, not solely based on where it is today."

Understanding Enterprise Risk Management: An Emerging Model for Building Shareholder Value, KPMG, December 2001

KPMG's Assurance & Advisory Service Center understood early that value and risk go hand in hand and that performance and risk management should converge to create, enhance and protect stakeholder value. In May 2007, the Institute of Management Accounting further characterized Enterprise Risk Management as aligning strategy, processes, technology, and knowledge with the purpose of evaluating and managing the uncertainties the enterprise faces as it creates value. It considers ERM to be a truly holistic, integrated, forward-looking, and process-oriented approach to managing all key business risks and opportunities—not just financial ones—with the intent of maximizing stakeholder value as a whole.

A. Oracle's Stance on Risk Management Platforms

Supporting these viewpoints, Oracle believes that proper risk management maximizes opportunity while mitigating and avoiding threats. Organizations need to have a distributed, dynamic and defined process for risk management instead of the fragmented and ad-hoc activities that are currently the norm. Oracle therefore helps organizations build a risk management program that is:

- **Holistic** – manage all categories of risk throughout the enterprise with a single platform to provide a complete 360° view of risk
- **Predictive –** foresee the onset of unacceptable levels of risk using automated and intelligent monitors on daily business operations
- **Relevant –** embed risk management into strategic and operational planning to proactively manage the impact of uncertainty on the achievement of organizational objectives

Today, organizations perform a number of different management activities to reduce the level of risk and uncertainty they face. In principal, these activities fall into two categories: Enterprise Performance Management (EPM) and Governance, Risk, and Compliance (GRC). EPM comprises processes to report, analyze and monitor current and past activities as well as the strategic, financial and operational simulation and planning activities to project potential future outcomes. GRC identifies and analyzes risk specific to achieving operational objectives, ensuring critical processes are properly controlled.

In other words, while EPM focuses on identifying how the opportunities and chances at hand can be turned into sustainable success, GRC strives to uncover what opportunities and threats are looming or already exist, which factors influence them, and how they can best be treated. The combined approach comprehensively looks at risk factors and drivers in and outside the organization to understand the potential positive or negative impact to the business. By then integrating risk into business planning, better strategic and operational decisions are taken on a daily basis and the bearing of uncertainty on the attainment of organizational goals is minimized.

B. Balancing Risk and Performance in an Integrated Platform

To achieve management excellence, a balance between performance and risk is therefore essential. Based on the Strategy-to-Success (S2S) framework that Oracle has defined with academics, analysts, partners and customers[1], risk and performance are managed in concert.

As an extension of Michael E. Porter's concept of defining an organization's value chain across its business processes, the S2S framework expands the scope including the stakeholder environment, market model and business model. It consists of six steps, in which the output from one becomes the input for the next:

- Understand the Stakeholder Environment
- Create a Market Model
- Develop the Business Model
- Create the Business Plan
- Monitor Business Operations
- Deliver Business Results and Provide Feedback to Other Processes

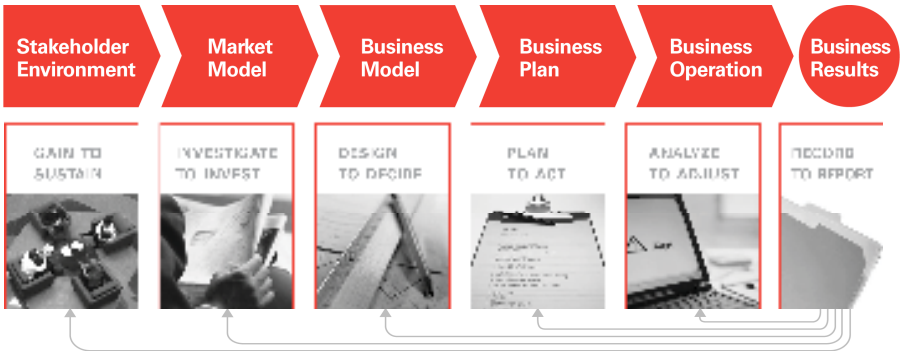

Figure 1: Strategy-to-Success Framework: The Management Process Value

[1] Management Excellence: How Tomorrow's Leaders Will Get Ahead, September 2008, www.oracle.com/solutions/business_intelligence/docs/management-excellence-whitepaper.pdf

As organizations progress through each step, GRC processes should also be integrated to ensure the integrity of business operations:

- Put in place controls over applications and technology
- Align policies and processes to best practices and control frameworks
- Identify and assess risks
- Report on key risks to business goals

For instance, when EPM and GRC converge, environmental or regulatory compliance are properly addressed because key stakeholders, their contributions and requirements are identified and market dynamics have been evaluated. The right investment decisions in new portfolios or market segments are made based on the evaluation of current market conditions, potential future changes, and overall market risk. Strategic risk management becomes more pertinent in the context of a business model and business plan for which strategic goals, targets, assumptions and risks have been translated into executable plans. Operational risks are clearly identified and adequately managed because business activities are monitored and the right adjustments are made to plans, budgets and forecasts. Internal controls appropriately expose exceptions, deviations and performance gaps and ensure the smooth conduct of business operations.

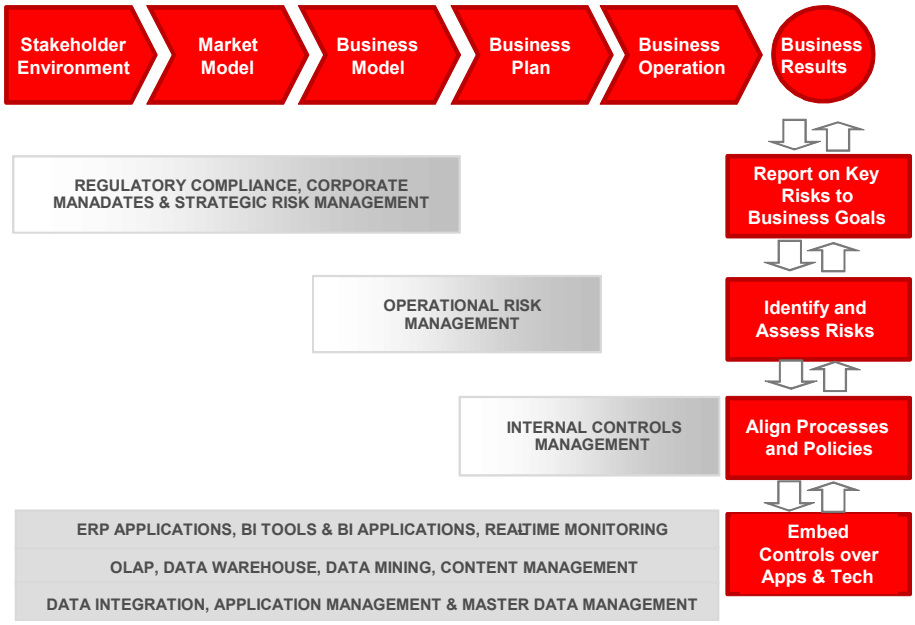

Figure 2: Balancing Risk and Performance based on the Strategy-To-Success Framework

When EPM and GRC meet and work together in a risk management platform, technology enables organizations not only to spot but also respond to and anticipate risk. Role-based dashboards and reports deliver the necessary entity-wide understanding of risks. Through continuous monitoring and automated alerts, emerging risk exposures are promptly identified. Risk treatments can then be modeled and the impact of each treatment analyzed before deciding on the appropriate course of action.

In addition, investors and regulatory bodies can rest assured that controls are in place to properly manage risks underlying critical business initiatives. Oracle's risk management platform provides automated controls to ensure the integrity of business processes and information, enforce proper segregation of duties and access controls for all systems and shorten remediation and attestation cycles with closed-loop risk reporting, treatment and monitoring.

In this way, a consistent and disciplined process for managing risk can be achieved with Oracle's comprehensive risk management platform. All types of risks across all levels of the organization are documented in a single platform. Risks are accurately assessed with the right mix of qualitative and quantitative measures. By then including risk assessment in business planning, the quality of strategic and operational decisions and the predictability of business results are enhanced.

In short, as an integrated EPM+GRC approach, risk management contributes to the successful achievement of business objectives and results by ensuring transparency in business operations. Business strategy is also sounder when adjusted to critical risk factors. As a result, organizations must explicitly and holistically manage risk if they wish to survive and create stakeholder value.

V. SUMMARY

Recent economic volatility has given risk management a new focus and eminence. The strongest companies are the ones that are able and willing to adapt, who actively integrate risk management as a critical factor at all levels of management process from strategy to success.

Regrettably, organizations have been hampered by pitfalls in traditional approaches to risk management. Seen as a back-office function, risk management may be limited to annual assessments that are not integrated with strategic and operational planning. Without the ability to apply a common taxonomy and weighting for different risk categories, organizations are forced to manage risk in functional silos, unable to see the interconnected nature of multiple risk events. Internal control and external risk transfer methods are largely manual, leaving firms open to unnecessary exposure.

By combining key capabilities of its market-leading EPM and GRC applications, Oracle delivers a solution that facilitates the establishment of clear criteria for an organization's risk appetite and institutes a disciplined process for the ongoing monitoring, evaluation, and control of risk. The combined solution identifies opportunities for value creation while also protecting against potential threats.

The 18th century theologian William Shedd remarked "a ship is safe in harbor, but that's not what ships are for." Likewise, businesses must take on risks to survive and thrive. A clear-headed identification of acceptable risks and a focus on the forward indicators that presage these risks are therefore essential.

Risk Management: Protect and Maximize Stakeholder Value
February 2009
Author: Stephanie Maziol

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com