Perspectives on ERM and the Risk Intelligent Enterprise™

Enterprise Risk Management Benchmark Survey
Table of contents

Executive summary ........................................................................................................ 1

Background and key themes .......................................................................................... 4

About this survey ............................................................................................................ 6

The current state of ERM ............................................................................................ 7

Benefits of ERM .......................................................................................................... 9

Challenges of ERM ....................................................................................................... 11

Characteristics of organizations that are prepared to manage risk ......................... 13

Implementing ERM and organizational approaches ................................................. 15

Conclusion .................................................................................................................. 27

Contacts ...................................................................................................................... 28

Executive summary

There has been a significant increase in interest in Enterprise Risk Management (ERM) and many companies are asking for comparative benchmark data on ERM, including program goals, responsibilities, organization structure, and implementation tools.

In response, Deloitte launched an ERM Benchmark Survey. The goal of the survey was to capture and report feedback on the current state of ERM implementation for a cross-section of companies and industries (excluding Financial Services). This information has now been compiled to develop profiles of what companies are reporting as either leading or prevailing ERM practices.

Companies were invited to participate in the survey during a series of roundtables and conferences held by Deloitte in North America. Other companies were invited through direct communication as representatives of selected industries. There were 151 company responses from North America, South America, and Europe representing consumer business, energy, manufacturing, process industries, and telecom and media. Most of these companies are midsized companies with annual revenues between $1 billion and $20 billion.

Please note that this is not a scientifically structured survey; rather, it is intended to provide a snapshot of current ERM perceptions and practices among a limited set of survey participants.

In this survey, ERM refers to the people, tools, processes, systems, and structures to improve risk intelligence, risk management capability, and competitive advantage. Risk Intelligence is the enterprise’s integrated capability to gather, analyze, interpret, and deploy responses to the critical risks to the enterprise.

Some key themes about ERM that emerged in the survey are:

1. Interest in ERM is growing, but 56% of respondents have had ERM programs in place for less than two years.
2. Regulation and regulatory compliance appear to be key drivers of ERM.
3. There is confusion about what ERM really means.
4. The primary goals of current ERM programs emphasize process and structure over outcomes.
5. Risk has not yet been fully incorporated into core business decision-making processes, such as strategic planning, capital allocation, and performance management.
6. The combination of lack of understanding of the benefits of ERM and difficulty in proving the business case is the biggest challenge facing ERM proponents.
7. The majority of respondents are not confident in the level of their organization’s preparedness for mission critical risks.
8. Europe is further ahead in ERM deployment.
9. Organizations that report that they are better able to manage risk have a more structured approach that has been in place for two years or more.
10. Current ERM programs are typically focused on risks to existing assets and miss the connection to future growth.
1. Interest in ERM is growing but 56% of respondents have had ERM programs in place for less than two years.

Respondents reported their organizations’ interest and investment in ERM as greater than it was a year earlier. Only very rarely did respondents describe their organization as having less interest than it did a year earlier. With 56% of companies having an ERM program in place for less than two years, most ERM programs are in relatively early stages of development. See Exhibits 2 and 15.

2. Regulation and regulatory compliance appear to be key drivers of ERM.

Respondents state that their organization’s ERM efforts are being driven, for the most part, by the need to be able to respond effectively to regulation (either because it is required by regulation as it is in Europe or because ERM is seen as a means to manage increasingly complex multijurisdictional compliance requirements). Typically, this characteristic is found in organizations whose ERM programs are at the early stages of maturity and who have not yet recognized the role ERM can play in value creation. This finding may also reflect the bias of the survey respondents who typically represent functions that are more closely aligned with regulation and compliance than business functions.

The key groups driving ERM within organizations are boards and audit committees, followed by internal audit and then senior management. Where regulation and compliance appear to be the primary drivers of ERM, operating management is not the key program driver. Senior management may be more interested in value creation (which is more closely linked to their compensable metrics) than in the protection of existing assets.

Of those respondents who stated that their companies had fully deployed ERM programs, the majority were in regulated industries, e.g., telecom and pharmaceuticals. See Exhibits 3, 14, and 17.

3. There is confusion about what ERM really means.

As with many approaches still in their relative infancy, there is much confusion about what is meant by ERM. Organizations are struggling with defining their programs, where and how to start, and how to demonstrate the value of improved risk management. Demonstrating the value of prevention is always a tough challenge. Management is demanding proof of the value proposition of ERM, just as they did when quality initiatives were first being introduced. Unfortunately, such proof is usually most evident after a catastrophe. See Exhibit 8.

4. The primary goals of current ERM programs emphasize process and structure over outcomes.

Identifying and reporting on risk and establishing a risk governance structure appear to be the primary goals of current ERM programs. Much lower ranked are outcome-related goals, such as improving preparedness to mitigate risk, protecting shareholder value, and minimizing the likelihood of catastrophic events. Other process issues, such as ensuring consistent policies and processes; integrating risk management into core business processes; and identifying risk interrelationships or opportunities across business units received low scores. While it may be that goals of fledging programs tend to focus more on process rather than with outcomes, failure to make such connections may have a large role to play in difficulties in convincing operating management of the relevance of ERM. See Exhibit 4.

5. Risk has not yet been fully incorporated into core business decision-making processes, such as strategic planning, capital allocation, and performance management.

Risk management functions, such as Internal Audit, Treasury, Insurance, Sarbanes-Oxley (SOX), Environmental Health & Safety (EH&S), and Legal report that they have more systematically incorporated risk into their decision-making processes. However, critical decision-making processes relating to future growth, e.g., Delegation of Authority Project Management, Strategic Planning, Mergers and Acquisitions, Capital Allocation, and Performance Management are less likely to systematically incorporate risk information into decision making. See Exhibit 7.

6. The combination of lack of understanding of the benefits of ERM and difficulty in proving the business case is the biggest challenge facing ERM proponents.

The lack of understanding of the benefits of ERM makes it very difficult to demonstrate value and, therefore, to gain support from management. Demonstrating the value of prevention is always difficult. Ultimately, the real value of ERM is as a tool for enterprise management (EM), not just risk management. Companies make money by taking risks that pay off and avoiding risks that do not. They must protect the value of their existing assets and create new value through growth. By implementing a more systematic approach to risk management through improved risk intelligence, companies will add an important and valuable tool to EM. See Exhibit 8.
7. The majority of respondents are not confident in the level of their organization’s preparedness for mission critical risks.

When asked to rate their organization’s preparedness to manage mission critical risks, and their confidence in their current level of preparedness, only 35% of respondents say that they are “highly confident” in their level of preparedness. This highlights the opportunity that a more systematic approach to ERM implementation may provide the needed means for improved preparedness. See Exhibit 9.

8. Europe is further ahead in ERM deployment.

European companies report the highest number of ERM programs that have been in place four years or more (43%). European Corporate Governance (CG) regulations have been in place for a decade, some for even longer. The European CG regulations also define a broader scope for ERM that includes the management of risks to strategic, operational, financial, and compliance objectives. See Exhibit 15.

9. Organizations that report that they are better able to manage risk have a more structured approach that has been in place for two years or more.

Organizations that report being better prepared to manage risk display a number of common characteristics:

- Specific responsibility for ERM has been assigned to a member of senior management.
- ERM is structured as a separate and independent function.
- ERM programs have typically been in place longer.
- ERM programs are fully operational (although there is some question about what that really means). See Exhibits 10 to 13.

10. Current ERM programs are typically focused on risks to existing assets and miss the connection to future growth.

Most ERM programs currently focus on risks to existing assets. These typically include risks to financial reporting and compliance and operations, such as business continuity, operations, inventory, treasury, insurance, etc. This is the traditional domain of risk management and it is certainly important. Unfortunately, such an approach does not typically address risks to future growth and, as such, may fail to capture the interest of operating management. These risks are unrewarded in the sense that no premium is obtained for managing them. There is only the potential for loss.

Rewarded risks are those that have more to do with strategy and its execution. These typically include the development of new products, entry into new markets, or acquisitions. These strategies hold the potential for gain and reward if they are intelligently managed, but they can have serious negative effects if they are not. One of the key themes that emerged in this survey is that current ERM programs give cursory attention to rewarded risks and focus primarily on the unrewarded risks related to asset protection. Certainly, the protection of existing assets is important and necessary, but it is not sufficient for future growth — and therein may lie the source of the disconnect with operating management.

There are not a lot of known examples that a company’s ERM program has been instrumental in allowing the organization to take advantage of market opportunity that has subsequently provided a tremendous boost in shareholder value, although it may be implicit in their ERM approach. There are, however, numerous examples of enterprises that have sustained major value losses due to their failure to properly anticipate and manage risk. For an increasing number of organizations, fear of this type of failure will hopefully prove to be sufficient incentive to implement and sustain ERM. However, ERM should not be interpreted as simply a prescription to be more risk averse. Calculated risk taking is essential for competitive advantage and growth. The real challenge is to become smarter about the risks that need to be taken, and those that need to be avoided, and how best to manage them. We call this risk intelligence. See Exhibits 5, 6, and 19.
Background and key themes

The management of risk is inherent to the survival of mankind. When early man built a fire at night to ward off predatory animals while he slept, he was managing risk. All of us manage risk on a daily basis, often without being aware we are doing it.

Risk management is not new but ERM, an approach to managing risk, is relatively recent. Risk Intelligent Enterprises™ manage risk for two reasons: to protect what they have and to grow the value of what they have. The premise of ERM is that it attempts to present an overall and integrated view of the risks to which an enterprise is exposed. Ideally, with this information, the enterprise is then able to make better informed decisions about how it can protect what it has and how it can, in an intelligent manner, add value to what it has. In other words, the organization can be smarter about the risks it needs to take. It can be “Risk Intelligent.”

ERM is an enabler of risk intelligence, and its true value may lie in its ability to enable the systematic identification of possible causes of failure — failure to protect existing assets and failure to achieve future growth, i.e., manage both unrewarded and rewarded risk. Unrewarded risks are typically associated with lack of integrity in financial reporting, noncompliance with laws and regulations, and operational failures, i.e., there is no premium to be obtained for taking these types of risks. Rewarded risks are those that typically have to do with strategy and its execution.

The extent to which an organization uses risk information from its ERM framework to influence decision making in both areas (unrewarded and rewarded risk) is a direct reflection of the maturity of its ERM program and of its risk intelligence.

The respondents in this survey, for the most part, indicate that their organizations are using the information from their ERM programs to deal with unrewarded risks. This is the traditional domain of risk management because it focuses on the protection of existing assets. An ERM program may only reach its true potential (and its greatest value) when it is used both as a tool to minimize unrewarded risk and to optimize strategy and execution (rewarded risk).

When examining the key themes that have arisen from this survey, it is important to examine the current ERM landscape. This landscape influences, to a large degree, the way in which the survey answers must be considered and any conclusions drawn.

The ERM landscape

What is ERM?

First of all, across respondents there was no clear agreement on what is meant by ERM. There are widely divergent opinions on what ERM is and who should be involved. In fact, even those organizations that have tried to set ERM standards, such as the Casualty & Actuarial Society, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), The Institute of Internal Auditors (IIA), and the Treasury Board Secretariats of numerous countries all have widely varying definitions.

Common ERM Elements

The key premises of ERM are that 1) risks are understood and managed across the enterprise, 2) there is a common language and increased awareness and dialogue about those risks that need to be taken for competitive advantage and those that need to be avoided, and 3) ultimately, decision makers are better equipped to make calculated choices about risk and reward in an increasingly complex and uncertain business environment.

Since risk management is so fundamental to management, most, if not all, organizations assert that they are already managing risk on an enterprise-wide basis. The problem is that what one respondent calls ERM, another may not. There are differences not only in how ERM is defined, but also in how it is deployed. Although some report that they are employing ERM, their efforts are not coordinated or integrated across all risk areas. Therefore, even among those who assert that they are using ERM, it is virtually impossible to get an “apples to apples” comparison.

Common metrics are lacking

There are currently no formal, agreed-upon industry metrics to assess risk within an ERM framework. Without a standard yardstick by which to quantify, measure, and aggregate risk information, the outcomes may be relevant to a specific organization but are not particularly useful in an “across-the-board” comparison.

ERM motivation and capability maturity differs by region

In Europe, ERM appears to be far ahead of the United States for a number of reasons. First, there are strong governments in Europe that have, for the most part, accepted and embraced the ERM concept. Second, far-reaching regulation (some of which requires the identification, assessment, and allocation of capital reserves for operational risk) influences the speed at which ERM is adopted. Even private, nonfinancial services companies in Europe appear to be moving quickly to implement ERM programs. Once they have complied with regulation, European companies seem to choose to exploit ERM as a value enhancer (a driver of tomorrow’s value), a move that could be considered characteristic of more mature ERM frameworks.

In the United States, where ERM appears relatively immature, the need to find a logical, all encompassing, efficient way of responding to the rising costs and complexities of multijurisdictional regulation might be the key driver. Yet it may be some time before U.S. organizations use the information from their ERM frameworks as the basis for strategic decision making. Most organizations in immature ERM environments tend to focus on process rather than output and outcomes and on the protection of existing assets versus future growth.
The high cost of compliance…and noncompliance
Maurice Chevalier, the French singer and actor, once said, “Old age is not so bad when you consider the alternative.” The same might be said of the cost of compliance and the higher cost of noncompliance. While the costs of noncompliance have not been systematically documented, the cost (and the consequences) of noncompliance have the potential to well exceed the cost of compliance.

Practice doesn’t always make perfect
Nothing stands still. The more complex an organization becomes (e.g., globalization, offshoring, third-party partnerships, vendor alliances, etc.) the more risks the organization is exposed to and, therefore, the more potential for failure. In other words, the ERM framework must keep pace (in terms of providing useful risk information) with the increasing complexity of the organization and its operating environment. As a clear example, despite their prior claims of sophistication, many financial institutions recently found themselves unprepared for the domino effects of the subprime crisis.

Investment in prevention is always a hard sell
Just ask any health care professional if prevention is an easy sell.

Boards are increasingly concerned about the personal responsibilities of due care and due diligence. For these reasons, they are asking more questions of management about the nature and level of risk to which their companies are exposed. A rational person need only look to the carnage associated with failure to manage risk, to be convinced of the need to be more diligent about understanding and where possible, preventing it.

ERM is really about enterprise management. Increasingly the case is being made for ERM as a tool for strategic advantage, such as in the case of the optimal allocation of capital to allow an organization to take advantage of market opportunity. The “catch 22” is that ERM cannot prove its strategic role until it is implemented and has been used for a period of time, but it cannot be sold to executive management without proof that it is a good investment.

Is ERM just a fad?
Some people have suggested that ERM is a fad. The same thing was said of Total Quality Management (TQM), the quality initiatives that originated in the 1950s and reached a peak in the 1980s and has since evolved into Six Sigma and Lean Manufacturing.

W. Edwards Deming, one of the foremost proponents of quality principles, maintained that it took at least seven years to change organizational culture.¹ For those organizations that had the determination — and the patience — to see it through, TQM and its successors have paid off. But for those organizations who have not supported TQM at the top and whose resolve has weakened over time, TQM may be considered a failure, one that has resulted from trying to implement a “fad.”

The recent spate of supply chain quality problems is an important reminder of the essential need to manage quality. Like quality once was, so is ERM today. Value needs to be demonstrated and that requires metrics. Nonetheless, the faster ERM is incorporated into the enterprise’s core business processes; the more likely it is to be both successful and sustainable.

But it is hard to imagine that any future model would scrap the main premise of ERM — the move away from managing risk in silos towards an enterprise-wide view of risk so that risk decisions are better informed. Just as globalization has exposed us to a new world view, new opportunities and new risks, ERM has exposed us to a new enterprise-wide view — and there may be no going back.

About this survey

The objective of this ERM Benchmark Survey is to provide a broad perspective on the state of risk management across a variety of industries, excluding financial services.¹

The benchmark survey, from which the findings are taken for the basis of this report, was conducted online during 2006 and 2007. A wide variety of industry groups are represented with the heaviest concentration in consumer business, energy, manufacturing, process industries, and telecom and media.

Respondents were from Europe, North America, and South America and most represent mid-sized companies with annual revenues between $1 billion and $20 billion. By far, the function most represented by respondents is Internal Audit Director/Manager (35.1%) with the next largest category (33.8%) comprised primarily of risk managers, directors, ERM leaders, project leaders, or coordinators. Chief Risk Officers (CROs), Controllers, and Chief Financial Officers (CFOs) account respectively for 8.6%, 6%, and 5.3% of respondents, while executives, such as Chief Executive Officers and Chief Operating Officers (COOs), each represent only 1% of respondents.

This survey is based on self-assessments. Self-assessment, by definition, entails an unknown degree of subjectivity, and Deloitte did not attempt to validate the responses. In addition, there is no statistical significance to the responses—they are merely the opinions held at the time by those who responded. It is also important to emphasize that prevailing practice is not necessarily “leading practice.”

Exhibit 1 provides a detailed breakdown of the characteristics of the organizations that participated.


² There are numerous examples of practices that arise simply because they fulfill a need at the time; when knowledge and sophistication increase, such practices are typically replaced with improved methods. Therefore, prevailing practice is not necessarily good practice.

Exhibit 1 — Profile of participating companies

<table>
<thead>
<tr>
<th>Industry</th>
<th>Listed</th>
<th>Nonlisted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aviation and Transport Services</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Consumer Business, including Consumer Products, Retail, Wholesale, and Distribution</td>
<td>23</td>
<td>9</td>
</tr>
<tr>
<td>Energy and Resources, including Oil and Gas, Power and Utilities, and Mining</td>
<td>21</td>
<td>8</td>
</tr>
<tr>
<td>Life Science and Health Care, including Pharmaceuticals, Health Plans, Health Care Providers, and Medical Devices</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Manufacturing, including Aerospace and Defense, Automotive and Diversified Manufacturing</td>
<td>23</td>
<td>6</td>
</tr>
<tr>
<td>Media and Entertainment</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Process industries, such as Chemicals and Paper</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>Public Sector, including Federal, State, and Municipal Governments</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Technology, including Semiconductor and Software</td>
<td>15</td>
<td>1</td>
</tr>
<tr>
<td>Telecommunication</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>Real Estate, including residential and commercial construction and REITS</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Other</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Note: Number of participants equals the number of the companies as there was only one survey participant per company. Total of participants split by industry adds up to more than 151 because some companies are in multiple industries.
The current state of ERM

The survey revealed that there is growing interest in ERM, a finding that is supported by the burgeoning number of articles on the topic in the business press and on the Internet. The vast majority of respondents indicate a growing interest in ERM or at least as much as there was a year earlier, a pattern seen consistently across Europe, North America, and South America. The majority of respondents (64% in Europe and 62% in North America) have a higher interest in ERM than they did a year earlier, with South America showing the greatest increase in interest, compared to that of the prior year.

However, as straightforward as this chart appears, the comparisons between regions — and even between organizations in the same region — are not necessarily “apples to apples.”

Regulation appears to be driving interest in ERM

This survey found that, by far, the biggest driver behind ERM in all three regions is regulation and regulatory complexity. European CG regulations have been in place for a decade, some for even longer (UK since 1992, Germany since 1998, France since 1995, and Netherlands since 1997). The European CG regulations also define a broader scope for ERM that includes the management of risks to strategic, operational, financial, and compliance objectives. In the U.S., regulation (SOX 2002) has focused less on strategic and operational objectives and more on the integrity of financial statements and the effectiveness of related controls. The New York Stock Exchange (NYSE) has also required changes to the role of the audit committee, including the responsibility to discuss with management, at least annually, its policies and guidelines for the management of all risk that constitute a major financial exposure.

Due to the growing volume of varied requirements (Foreign Corrupt Practices Act, privacy issues, employment and environmental statutes, CG, and other regulations) organizations should be looking for a holistic way to comply.

In addition, there is some rating agency influence building. Standard & Poor’s (S&P) and Moody’s have indicated, they will incorporate ERM assessment into the credit rating evaluation for all industries, in addition to financial services. In May 2008, S&P published a paper, “Enterprise Risk Management: Standard & Poor’s To Apply Enterprise Risk Analysis to Corporate Ratings.”

The second and third drivers of ERM in all regions are “other” and “unanticipated losses,” with unanticipated losses being the second driver in South America and the third in Europe and North America. As ERM programs mature, market drivers may move the focus from regulation to both value protection and value creation.

---

Primary ERM goals are to identify, measure, assess, and report on risk and create a governance structure

When asked to rank, in order of importance, the top 10 goals of an ERM program, the majority of respondents indicated that processes to “identify, measure, assess, and report on corporate-wide risks” (51%) and “create a risk governance structure to facilitate communication” (48%) were the top goals — rather than outcomes, such as “minimize likelihood or impact of catastrophic events” (31%) and “protect shareholder value” (33%). This thinking may be typical of programs that are still yet to be proven in terms of long-term benefits, with the focus on processes and structure rather than on outcomes.

The primary goals of ERM are risk identification (51%), governance structure (49%), alignment of risk with corporate objectives/strategies (45%), improved transparency (37%), and improved preparedness (36%).

The importance of integration of ERM into core business processes, such as strategic planning and coordination and consistency and management of interrelationships of risks (Exhibit 4), was ranked much lower. Although the responses fall within a 33% to 37% range, this outcome would appear to reflect the corresponding lack of emphasis on reducing the likelihood or impact of catastrophic events, an undertaking which typically requires cross-functional coordination. These findings may also account for the difficulty in demonstrating the value of ERM. It may also contribute to perceptions that ERM is not part of the core business and, therefore, is less relevant to the success of the business. By placing greater emphasis on process over outcomes, ERM practitioners may reduce management’s perceptions of relevance.

Exhibit 4 — Primary ERM goals are to identify, measure, assess, and report on risk and create a governance structure
Benefits of ERM

The top five experienced benefits are all excellent benefits. While the first three focus more on people and process, the latter two focus on vulnerability and related decision making and may be more related to the management of asset protection and unrewarded risks. These benefits may also reflect the early maturity phases of an ERM program. Given that 56% of those who responded to this survey represent organizations that have had an ERM program in place for only two years, further benefits may be still realized. However, remember that there are differences on the part of respondents in their definitions of what constitutes an ERM program.

Given the relatively early stage of development, the top five “expected” benefits seem to relate more to the management of future growth and potentially rewarded risk. This has a direct correlation to risk maturity — organizations begin by focusing on protecting assets and then, later use ERM information as the basis for decision making related to creating future growth and value.

The differences between early experiences with ERM and the expected future benefits highlight the need for a longer-term commitment to ERM programs, with the understanding that full implementation and maturity cannot be achieved overnight. Again, the challenge may remain in demonstrating the value before the program has been implemented.

Expected benefits may be somewhat at odds with program goals

There does appear to be some alignment between the highest ranked goals and expected benefits, such as aligning risks with corporate objectives and strategies (45%) and aligning risk appetite and strategy (44%). There also appear to be some inconsistencies between the highest ranked program goals and the expected benefits. Most obvious is the difference between the second lowest ranked goal of minimizing the likelihood of catastrophic losses (31%) and the expected benefits of minimizing operational surprises and losses (42%).

The goals of the ERM program will likely vary depending upon the maturity of the organization. For example, when the risk management system is driven by the board or its committees, it may be perceived by operating management as yet another form of compliance, something that “must be done” and not driven by business needs.
Risk functions rather than business functions have incorporated risk into their decision-making processes

The greatest value from an ERM program may be derived when an organization incorporates a systematic consideration of risk into its decision-making process, decisions related both to protection of assets and future growth. In the survey, respondents identify that, for their organizations, risk information is incorporated more systematically into the processes related to Internal Audit (52%), Treasury (41%), Insurance (37%), SOX (40%), EH&S (34%), and Legal (32%), all traditional areas of risk management whose primary focus is on the protection of existing assets rather than on future growth.

Respondents also indicate that core business processes relating to future growth, e.g., Delegation of Authority (25%), Project Management (23%), Strategic Planning (22%), Mergers and Acquisitions (2%), Capital Allocation (13%), and Performance Management (11%) are least likely to have systematically incorporated risk information into decision making. Although many of these latter functions are reported to have either partially incorporated or plan to incorporate risk consideration in the decision-making processes. These responses may reflect the bias of respondents who are largely from risk and compliance-related functions.

However, if risk is not systematically considered by the business functions, it is not surprising that one of the major obstacles to ERM is lack of understanding of the benefits (see Exhibit 8 — ERM Challenges). In order for operational management to see the value, they need to see their issues are being addressed in a beneficial way. The challenge is to show how more systematic consideration of risk can help operating management achieve their business objectives.

Exhibit 7 — Risk consideration in decision-making

Performance management, strategic management, and capital allocation decisions need to more systematically integrate consideration of risk to be meaningful to management. But the minds and hearts of senior executives will likely only be won when there is a demonstrated clear link between risk management and performance management. The value link does not yet appear to have been made as 40% of respondents indicate that there are no plans to link risk and performance. ERM may well be seen, at least by executives, as a means for avoiding rather than taking risk. Alternatively, if there is no linkage between risk management and performance management, then ERM really makes no difference where it counts most.
Challenges of ERM

When combined, lack of understanding of the benefits of ERM and difficulty in proving the business case is the biggest challenge

“Lack of understanding of the benefits of ERM” (46%) is very closely related to “Difficulty in proving the business case” (35%). When taken in combination, “demonstrating the value of ERM” is the biggest challenge facing ERM. If there is a lack of understanding of the benefits of the integrated management of risk, it is difficult to demonstrate value and, therefore, to gain support from management. Resistance to management buy-in may be compounded by a tendency of risk managers to focus on unrewarded risks to existing assets (necessary but not sufficient), while management’s priorities typically relate to future growth.

“Difficulty in measuring and assessing risks” and “time and costs required to implement” were also ranked as significant challenges. Initial efforts at risk assessment and measurement are often performed on a subjective basis, especially in the first years of ERM program implementation. Because ERM is new, there is a lack of data with which to measure/quantify risk. Intangible risks, such as those to reputation, for example, add to the difficulty of measurement.

Many respondents are also concerned about the “time and cost required to implement an ERM program,” as well as the “lack of in-house skills.” The time and cost of ERM implementation should be seen in the context and cost of failure to manage risks, including noncompliance. Concerns about cost and resource utilization will naturally be higher if the benefits are not well understood.

The level of ERM challenge comes down to the difficulty of proving the business case. By definition, a business case must take into account the time and cost required, as well as the benefits, all of which are difficult to quantify. As was initially the case with proving the value of quality, the costs of poor risk management (both existing assets and future growth) need to be compared to the costs of good risk management, including costs of prevention, preparation, response, and recovery. Management should weigh the benefits of risk-informed decision making based on an enterprise-wide view of risk compared with the drawbacks of making decisions based on siloed information.

The Catch 22 of ERM

The need to undertake ERM to prove its worth but the need to prove ERM’s worth before it is undertaken. But this is the problem with any form of prevention or preparedness — it is much easier to see the value once you have experienced the loss. This is the value of disaster recovery or insurance. If nothing adverse happens, then some may ask “why did we spend the money or why did we prepare for something that didn’t happen?” When such risks do occur, they are comforted by insurance and their recovery plans, or in their absence, wish they had the foresight to do so.

### Exhibit 8 — ERM challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Moderate or Significant Challenge</th>
<th>Not a Challenge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Difficulty in measuring and assessing risks</td>
<td>47%</td>
<td>5%</td>
</tr>
<tr>
<td>Time and costs required to implement</td>
<td>47%</td>
<td>5%</td>
</tr>
<tr>
<td>Lack of understanding of the benefits of the integrated management of risk across the enterprise</td>
<td>46%</td>
<td>6%</td>
</tr>
<tr>
<td>Lack of in-house skills</td>
<td>39%</td>
<td>12%</td>
</tr>
<tr>
<td>Lack of support among management</td>
<td>35%</td>
<td>17%</td>
</tr>
<tr>
<td>Difficulty in proving the business case</td>
<td>35%</td>
<td>15%</td>
</tr>
<tr>
<td>Higher/redundant cost for managing risk at both corporate and business unit level</td>
<td>31%</td>
<td>17%</td>
</tr>
<tr>
<td>Competing initiatives (e.g., SOX)</td>
<td>29%</td>
<td>19%</td>
</tr>
<tr>
<td>Regulatory or legal issues</td>
<td>20%</td>
<td>30%</td>
</tr>
</tbody>
</table>
Preparedness to manage mission critical risks

Almost 50% of respondents believe that their organizations are only somewhat prepared to manage mission critical risks

Respondents were asked to rate their organization’s preparedness to manage mission critical risks, as well as their confidence in their current level of preparedness. Only 50% of respondents believe that their organizations are “very well prepared” (8%) or “prepared” (42%) to manage mission critical risks. When asked, “where you believe your company is prepared, how confident are you in the current level of preparedness for its mission critical risks?,” only 35% said they were “highly confident” in their level of preparedness.

Nearly 50% of respondents identify that their organizations are only “somewhat prepared” to manage mission critical risks. Presumably, failure to manage a mission critical risk could mean the failure of the enterprise or at least very serious harm. This result should serve as a call to action. Clearly, there is a significant opportunity for improvement in preparedness regardless of whether or not they call it ERM.

Exhibit 9 — Preparedness for managing risk
Characteristics of organizations that are prepared to manage risk

Organizations that assessed themselves as being better prepared to manage risk report a number of common characteristics:

• Specific responsibility for ERM has been assigned to a member of senior management.
• ERM is structured as a separate and independent function.
• ERM programs have typically been in place longer.
• ERM programs are fully operational (although there is some question about what that really means).

A specific executive has been assigned responsibility

Responses indicate organizations that have assigned an individual executive responsibility for ERM report being better prepared to manage risk than those who have not. Sixty-four percent of respondents who had an executive assigned to ERM report, they are “prepared” to manage risk, while 36% state they are only “somewhat prepared.” Conversely, only 28% of respondents from companies that had no executive assigned to ERM describe their organizations as “prepared” while 72% indicate their organizations are “somewhat prepared.”

Note: This survey did not include any means to validate whether these organizations are actually better prepared compared to the others.

ERM is a separate function

Respondents report that if ERM is a separate, independent function in their organization, they feel “better prepared” to manage risk than those organizations that tend to lump ERM in with another function. Sixty-nine percent of respondents whose organizations have established ERM as a separate function indicate feeling “prepared” to manage risk versus only 46% of respondents whose organizations have lumped ERM in with another function.
Preparedness relates to the length of time ERM has been in place

There is a vast difference (nearly 60%) in reports of preparedness between those respondents who indicate that their ERM program is under a year old and those who indicate their ERM program is at least four years old. In fact, 100% of respondents with more established ERM programs report being “prepared” to manage risk, illustrating that their sense of preparedness increases with time. In keeping with previous findings, risk capability maturity is linked to being prepared to manage mission critical risk. This is an important conclusion and may justify a more structured approach toward rewarded risk.

Operational status of ERM

Following closely on the findings in Exhibit 13, respondents who state they have fully operational ERM programs, report being better prepared to effectively manage risk compared to those with programs that are not fully operational.

ERM programs do not appear to significantly enhance preparedness until they are fully operational. Reports of readiness to manage critical risks directly correlates with taking the steps necessary to fully formalize and operationalize ERM.
Implementing ERM and organizational approaches

Key survey outcomes related to ERM implementation

Industry, region, and listing status
1. Regulated industries report higher levels of full ERM deployment.
2. Europe is further ahead in ERM deployment.
3. Almost as many unlisted versus listed companies are considering ERM.

Organization
4. Boards are the primary drivers of ERM.
5. Only 35% of companies have adopted a specific ERM standard.
6. Current ERM frameworks tend to focus most on compliance and asset protection risks.
7. Initial ERM implementation focus is on policy, process, and structure.
8. CFOs and CROs have primary responsibility for ERM.
9. CROs usually report to the CFO or CEO.
10. The primary responsibilities of the CRO are risk analytics and monitoring exposure versus limits.
11. Boards are usually updated on risk quarterly and annually.

12. The audit committee typically oversees ERM.
13. Most risk management committees (RMC) are management not board committees.

Policies
14. Only 2% of companies train a broader group of employees in risk management.
15. Few companies have defined their appetite for risk, their risk tolerances, or developed early warning or escalation procedures.

Processes
16. Only 18% have fully implemented a risk dashboard or reporting process.
17. Eighty-one percent use probability, but only 18% are highly confident in the results.
18. Self-assessment is the predominant risk measurement tool.
19. Risk assessments are typically conducted semiannually or quarterly.

Systems
20. Approximately 27% are using technology/software tools to monitor risk.

1. Regulated industries lead full ERM implementation.

Certain sectors are further along than others in deploying ERM

Given that regulation and regulatory complexity appear to be the number one drivers of current ERM programs, respondents in regulated industries report that their ERM programs are more fully deployed. Telecommunications (38%), life science and health care (34%), and energy (24%) are more likely to have fully operational ERM programs than those industries that are less regulated, such as media and entertainment (12%).

Even though the chemicals and paper industry (14%) is subject to much regulation, it is not a regulated industry. This may account for its comparatively low rate of deployment. In addition, the chemicals industry already has risk-based systems (e.g., health and safety systems/programs), which are not typically considered to be ERM programs.

---

Even though the chemicals and paper industry (14%) is subject to much regulation, it is not a regulated industry. This may account for its comparatively low rate of deployment. In addition, the chemicals industry already has risk-based systems (e.g., health and safety systems/programs), which are not typically considered to be ERM programs.
2. Europe is further ahead in ERM deployment.

The region with the largest percentage of organizations that have had an ERM program in place for more than four years is Europe. This is not surprising given that regulation is one of the key drivers of ERM in Europe where regulation requires risk-assessment programs.

CG regulations are relatively new to the U.S. (since 2002). South America, Mexico, and Brazil have CG regulatory requirements but these are also more recent than the European statutes.

Culture plays a role in regional differences between ERM programs, and there appears to be systemic differences between North America and other regions.

![Exhibit 15 — Regional differences between ERM programs](image)

3. Almost as many unlisted versus listed companies are considering ERM.

Whether a company is listed or not listed appears to have influenced how developed its current ERM program will be. Respondents report twice the percentage of listed companies (listed: 26%; nonlisted: 13%) that have fully operational ERM programs. Interestingly, there is no significant difference between listed and nonlisted companies, as it relates to “in development” or “considering developing” an ERM program (61% versus 59%). This may reflect the growing recognition that a more systematic approach to risk management is simply good business and not just a regulatory compliance.

The higher level of fully operational ERM programs in listed companies may be explained by greater regulatory requirements for listed companies, including, of course, listing requirements themselves.
4. Boards are the primary drivers of ERM.

ERM, at present, appears to be pushed, not pulled, through organizations. Respondents report that in their organizations, the board, including the audit committee, jointly accounts for at least 31% of the “champions” who push for ERM within an organization. Boards serve as an oversight function and internal audit (21%) provides independent assessment and monitoring services. However, senior management primarily determines how effectively and efficiently risk is managed across the organization. Yet senior management is perceived as driving ERM in only 18% of cases, but when combined with “all of the above,” the level rises to 39%.

Clearly, operating management has the power to pull ERM through the organization. If there is reluctance to embrace ERM, it may be due to a possible disconnect between program goals (asset protection) and expectations (value creation). It may also be that management’s agenda is more aligned to future growth and management is, therefore, less inclined to actively support asset protection. The goals of audit committees and risk management professionals appear to be different from operating management’s, which may contribute to reduced management support for a more systematic approach to risk. As noted earlier, it may also account for why risk is not systematically considered in such core business processes as strategic planning, capital allocation, and performance management.

5. Only 35% of companies have adopted a specific ERM standard.

Almost as many respondents report that their organizations have chosen a specific standard (35%) as those who report that their organizations have not chosen a specific standard (37%). However, 28% left the question blank, indicating that they may not know. Of those using a specific standard, COSO ERM is, by far, the most popular.

If a specific standard has not been adopted, there may be a lack of consistency across the enterprise in ERM terminology, strategy, and approaches, which may further compound difficulties in establishing value. It is also possible that some of the immaturity observed in ERM programs may be tied to the lack of adoption of a standard framework.
6. Current ERM frameworks tend to focus most on compliance and asset protection risks.

### Exhibit 19 — Types of risk managed within ERM frameworks

<table>
<thead>
<tr>
<th>Risk Type</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal/regulatory/environmental changes</td>
<td>55%</td>
</tr>
<tr>
<td>Legal and regulatory compliance</td>
<td>53%</td>
</tr>
<tr>
<td>Business continuity (natural disasters/severe weather/suppliers)</td>
<td>49%</td>
</tr>
<tr>
<td>Economic conditions/trends</td>
<td>46%</td>
</tr>
<tr>
<td>Liability/litigation</td>
<td>46%</td>
</tr>
<tr>
<td>Production (quality, supply, stability, sourcing, and costs)</td>
<td>44%</td>
</tr>
<tr>
<td>Financial statement integrity</td>
<td>44%</td>
</tr>
<tr>
<td>Fraud, collusion/corruption</td>
<td>43%</td>
</tr>
<tr>
<td>Competitive actions (pricing, conveniences, services, or amenities)</td>
<td>42%</td>
</tr>
<tr>
<td>Computer controls</td>
<td>42%</td>
</tr>
<tr>
<td>Technology obsolescence</td>
<td>38%</td>
</tr>
<tr>
<td>Ability to attract, train, &amp; retain talent</td>
<td>38%</td>
</tr>
<tr>
<td>Market</td>
<td>38%</td>
</tr>
<tr>
<td>Credit</td>
<td>37%</td>
</tr>
<tr>
<td>Security</td>
<td>37%</td>
</tr>
<tr>
<td>Consumer demands/preferences</td>
<td>36%</td>
</tr>
<tr>
<td>Ability to develop/market new products</td>
<td>35%</td>
</tr>
<tr>
<td>Political stability/country risk</td>
<td>34%</td>
</tr>
<tr>
<td>Terrorist activities/war/civil unrest</td>
<td>34%</td>
</tr>
<tr>
<td>Liquidity</td>
<td>33%</td>
</tr>
<tr>
<td>Commodities</td>
<td>32%</td>
</tr>
<tr>
<td>M&amp;A strategy/execution/integration</td>
<td>31%</td>
</tr>
<tr>
<td>Achievement of cost reduction objectives</td>
<td>31%</td>
</tr>
<tr>
<td>Capital accessibility/availability</td>
<td>30%</td>
</tr>
<tr>
<td>Intellectual capital issues</td>
<td>29%</td>
</tr>
<tr>
<td>Privacy</td>
<td>26%</td>
</tr>
<tr>
<td>Alignment of incentives</td>
<td>17%</td>
</tr>
</tbody>
</table>

Consistent with the earlier finding that regulation and compliance is a key driver of ERM, with a few exceptions, current ERM programs typically focus on compliance and asset protection, i.e., unrewarded risk. The top 10 risks addressed in ERM include Legal and Regulatory Compliance, Business Continuity, Litigation, Production Quality, Financial Statement Integrity, and Fraud and Computer Controls. Typically, these are the domains of the risk specialties whose focus is to avoid or eliminate risk. Notable exceptions are economic conditions and trends, and competitive actions.

Unrewarded risk offers no premium and is most often associated with lack of integrity in financial reporting, noncompliance, and operational failures. This is the traditional domain of risk management because it focuses on the protection of existing assets. Rewarded risks have more to do with strategy and its execution.

The further one goes down the list in Exhibit 19, the more the risks are related to strategy and execution, e.g., ability to attract and retain talent; market, credit, and consumer preferences; ability to develop and market new products; capital accessibility/availability; mergers and acquisitions strategy; and intellectual capital issues and alignment of incentives.

This list would seem to be inversely related to operating management’s growth agenda. Accordingly, it is no surprise that operating management would question the value and applicability of ERM to their agenda, given this apparent disconnect.

This finding is further reinforced by a survey of emerging markets, *Innovation in emerging markets: Strategies for achieving commercial success*. This survey found that very few companies actually conduct a rigorous risk assessment before entering an emerging market. Even fewer continue to do so once they have entered the market.

---

[i][4] Innovation in emerging markets: Strategies for achieving commercial success, July 2006, Deloitte & Touche LLP – United Kingdom, [http://www.deloitte.com/dtt/cda/doc/content/uk_manuf_innovation_in_emerging_markets_jul06.pdf](http://www.deloitte.com/dtt/cda/doc/content/uk_manuf_innovation_in_emerging_markets_jul06.pdf)
7. Initial ERM implementation focus is on policy, process, and structure.

The chart above is consistent with earlier findings. The majority of respondents indicate that their organizations have implemented processes around tasks that are relatively “easy” — conducting formal, corporate-wide risk assessments, aggregating risks at the corporate level, developing corporate-wide risk policies and procedures, and developing an enterprise risk dashboard/reporting process.

However, once the “real” work begins, the percentage of respondents who indicate that the process is implemented for their organization, drops off dramatically. For example, 28% of respondents indicate that their organization conducts formal corporate-wide risk assessments on a periodic basis (process). However, that number drops to 8% when respondents are asked to assess whether their organizations have implemented a means to integrate risk management into other corporate practices, such as strategic planning, capital allocation, mergers and acquisitions, etc. This is characteristic of organizations that find the process part of ERM relatively easy and familiar, while the value components remain more unfamiliar and uncertain.
8. CFOs and CROs have primary responsibility for ERM.

Respondents indicate that the CFO plays a key role (34%). This may also explain why risk integration within the finance function is high. The next most common position assigned responsibility for ERM is the CRO (25%). There may be a movement toward more deliberate, focused oversight of ERM as the combination of CRO and director of ERM comprise 32% of responses. As will be seen in the next exhibit on reporting relationships, CROs typically report to the CFO.

The high percentage of “other” in this chart includes positions, such as the VP of Auditing and Compliance, various individuals in the legal department, and heads of CG. The CEO was identified in only 9% of cases.

9. CROs usually report to the CFO or CEO.

Of those organizations that have a CRO, respondents report that the majority of those positions report to the CFO (33%) or to the CEO (27%). High accountability and organizational visibility for the CRO may reflect a commitment to ERM from the top and helps set the stage for successful ERM programs.
10. The primary responsibilities of the CRO are risk analytics and monitoring exposure versus limits.

![Responsibilities assigned to the CRO]

Respondents identified that the primary roles of the CRO in their organizations are:
- Risk analytics and reporting
- Monitoring exposure versus limits

Approximately 40% of respondents indicate that CROs have primary responsibility for developing controls, policies, and monitoring compliance. Almost the same percentage indicates that CROs have primary responsibility for independent verification of risk methodology. The latter role could be a potential conflict if the CRO has any direct risk management responsibilities.

11. Boards are usually updated on risk quarterly and annually.

Respondents state that quarterly and annually are the most common cycles for updating the board with risk management information. Sixteen percent of respondents state that they update their board as requested.
12. The audit committee typically oversees ERM.

The audit committee charter is one way to formalize and communicate the board’s expectations of management when it comes to risk management. The NYSE requires that listed companies have a charter that details adherence to a variety of NYSE requirements. The audit committee charter is not required by organizations that are not listed on the NYSE; however, these requirements should nonetheless be considered good practice.

Respondents to this particular question were not asked to indicate whether or not the audit committee charter is a requirement of their NYSE obligations (in other words, whether or not they are listed on that exchange).

13. Most risk management committees are management, not board committees.

Forty percent of respondent organizations have a Risk Management Committee (RMC). Of those, the greatest number, 25%, indicate that their organizations have a management level-only committee, 10% have a board and management level RMC, and only 2% have a board level-only RMC.

Sixty percent of respondents have no RMC. This may reflect that an individual is in-charge of ERM, such as a CFO or a Director of ERM. These respondents may not see the need to form a committee.
14. Only 2% of companies train a broader group of employees in risk management.

Sixty-seven percent of respondents state their organizations train only those specialists who perform specific risk management functions. Survey respondents report that very few of their organizations regularly train a broader group of employees regarding risk management. This finding should raise a red flag, given one of the most desired benefits of ERM is a risk-aware culture and achieving this culture is often cited as a significant challenge to ERM implementation.

15. Few companies have defined their appetite for risk, their risk tolerances, or developed early warning or escalation procedures.

---

**Exhibit 27 — Scope of ERM training**

Sixty-seven percent of respondents state their organizations train only those specialists who perform specific risk management functions. Survey respondents report that very few of their organizations regularly train a broader group of employees regarding risk management. This finding should raise a red flag, given one of the most desired benefits of ERM is a risk-aware culture and achieving this culture is often cited as a significant challenge to ERM implementation.

**Exhibit 28 — Risk appetite**

---
A large number of respondents state that the questions related to risk appetite were not applicable to them. A small percentage of respondents (14%) state that their companies have defined the kinds of risks they are willing to tolerate. A smaller percentage (11%) indicates their organizations have defined the total risk exposures they are willing to accept. A still smaller percentage, (8%), state that they have a process for early warning. The same percentage of companies that have some form of process (partial or full) for monitoring when the risk appetite approaches or exceeds defined limits (early warning), also have a process (full or partial) for correction and escalation of these risks cases. This would appear to indicate that once you have defined the limits of risk you are willing to take, you must, by necessity, define corrective action.

16. Only 18% have fully implemented a risk dashboard or reporting process.

In order to satisfy a host of business and regulatory requirements, risk information needs to be presented in such a way that it is clear which risk event is being discussed, what the potential impact is for the company, and what actions have been planned and their status. The board and senior executive need to know the risk profile and changes within it, so they can have the necessary insight to fulfill their oversight responsibilities. One of the best ways to present this information may be through various dashboards.

Nonetheless, 28% of respondents indicate that their organizations are still considering, or have no plans to implement, a dashboard. This is in contrast to the earlier finding that management reporting was one of the top five benefits experienced.

An enterprise risk dashboard or reporting process is a key component of a risk intelligent organization. It will be much more difficult to make risk-informed decisions without this kind of intelligence.

Once the risks the organization is willing to tolerate have been defined, the level of acceptable exposure is less clear-cut. Fifty-three percent of respondents indicate their organizations have defined the kinds of risk they will tolerate but 42% of respondents indicate that their organizations have not yet defined the exposure they are willing to accept. This may be a product of maturity of the ERM program—many companies may be wrestling with how to deploy these concepts.
17. 81% use probability but only 18% are highly confident in the results.

Exhibit 30 — Risk assessment criteria

More than 65% of respondents report that they use inherent and residual risk. Inherent risk is the exposure before management intervention and residual risk is the exposure after management intervention. A full 81% of respondents state that their organizations use “probability of occurrence” to assess risk, but only 18% have high or very high confidence in this approach. Only 16% use “speed of onset.” While “probability of occurrence” is a common metric, severe, low-probability incidents should not be ignored. In light of recent events previously considered improbable, practitioners may have cause to reevaluate their use of probabilities.

18. Self-assessment is the predominant risk measurement tool.

Exhibit 31 — Risk assessment tools and methodologies

<table>
<thead>
<tr>
<th>Tools and Methodologies</th>
<th>Currently use?</th>
<th>Plan to use?</th>
<th>Which metrics pose the greatest challenge?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-assessments</td>
<td>41%</td>
<td>10%</td>
<td>2%</td>
</tr>
<tr>
<td>Economic metrics, such as value at risk, earnings at risk, cash flow at risk, RAROC, NPV/IRR, economic value added</td>
<td>33%</td>
<td>9%</td>
<td>3%</td>
</tr>
<tr>
<td>Scenario analysis</td>
<td>33%</td>
<td>11%</td>
<td>3%</td>
</tr>
<tr>
<td>Industry benchmarks/loss experience</td>
<td>26%</td>
<td>12%</td>
<td>3%</td>
</tr>
<tr>
<td>Key risk indicators</td>
<td>25%</td>
<td>15%</td>
<td>3%</td>
</tr>
<tr>
<td>Probabilistic analysis</td>
<td>25%</td>
<td>12%</td>
<td>2%</td>
</tr>
<tr>
<td>Third-party assessments</td>
<td>19%</td>
<td>12%</td>
<td>5%</td>
</tr>
<tr>
<td>Stress tests</td>
<td>15%</td>
<td>11%</td>
<td>4%</td>
</tr>
<tr>
<td>Quality tools, such as failure mode and effects analysis</td>
<td>14%</td>
<td>11%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Forty-one percent of respondents indicate that self-assessments are the most frequent means of measuring and monitoring risk. This is followed by economic metrics and scenario analysis as second most common. Benchmarking, key risk indicators, and probabilistic analyses are used by approximately 25% of respondent organizations. In contrast to the earlier finding that 81% of respondents used probabilities to assess risk, in this case only 25% report probabilities are used. Inconsistencies, such as these, point to the difficulties of measuring and monitoring risk. Least used were quality tools, such as failure modes and effects analysis.
19. Risk assessments are typically conducted semiannually or annually.

Respondents report that their organizations conduct enterprise risk assessments annually or semiannually (65%). However, frequency may be only a part of the story. Perhaps the more important issue is how it is done: whether it is manual versus automated, whether it is deep analysis versus a high-level update. There is an opportunity to leverage technology to help make ERM processes more efficient and effective. An overreliance on qualitative assessments is inevitably subject to bias and fatigue. It may be best to complement and corroborate qualitative assessments with quantitative data to the extent practical. Nonetheless, risk management is ultimately a judgment.

20. Approximately 27% are using technology/software tools to monitor risk.

Consistent with the prior finding that many risk assessments are qualitative, only 27% of respondents indicate that their organizations are using technology/software tools to monitor and manage risk on an integrated enterprise-wide basis. Unfortunately, the connection to future growth has not yet been made, as only 9% of respondents report their organizations are integrating ERM with Performance Management. This may mean that risk management is disconnected from other key management activities and, thus, disconnected from the value gained. Without this vital input, it may be virtually impossible to convince management of the value of improved risk management, since there is no linkage to value only loss.

With 67% stating that they do not use technology to monitor and manage risks, there appears to be plenty of room for improving the efficiency of ERM methodologies through technology.
ERM adoption and implementation appears to follow a somewhat predictable pattern. The first stage typically focuses on mandatory risk management processes associated with asset protection (unrewarded risks). The second stage addresses cross-functional coordination and integration. The third stage is to address risks to future growth (potentially rewarded risks). This later stage may more directly appeal to the goals and interests of operating management and thereby achieve its greater potential. It is not clear how long it takes an organization to reach this point and there are many factors that contribute to its success.

Those who have ever tried to learn a new software program recognize, at least in the beginning, that they often don’t come close to using or understanding the program’s full potential. Some, who are more adventuresome, may venture into unfamiliar territory in an attempt to gain more benefit. The majority, however, at least in the short term, prefer to stay safely within the confines of limited understanding and allow the program to fulfill basic requirements. As comfortable as it may be to stay within the confines of a limited understanding, this practice neither benefits the long term nor optimizes the investment in the software.

The same might be true of many organizations’ approach to an enterprise-wide program of risk management or ERM. The majority of those who say they have and use an ERM program appear to reside in the “safe zone” — the place where ERM is simply used to respond effectively to regulation (either because it is required by law or because it is seen as a way to manage compliance requirements). However, once the internal controls for financial reporting issues have been addressed, the resources and systems should be applied to more operational and strategic risks. As such, the ERM system can help management to understand and manage the risks in business assumptions, and the achievement of business objectives and strategies.

The findings of this survey confirm that ERM is being used, for the most part, to address asset protection-related risks and much less so to address risks to future growth. The connection to risks to future growth does not appear to have yet been made, as only a handful of respondents report that their organizations are integrating ERM with Performance Management. People can be told that ERM should be a management instrument, but when the driving roles are staff functions and without a clear cause and effect relationship between ERM and value gained, performance management, or compensation, it will be very difficult to convince anyone of the value.

So how does one go about making that happen?

As long as ERM is primarily seen as a means for asset protection (necessary but not sufficient) rather than value creation as well, the real value connection will not be made. As long as ERM remains an initiative separate and apart from the way the business is really run, the value will not be realized. The key is to recognize the potential contribution of ERM as a tool for Enterprise Management, not just risk management. By improving the risk intelligence of the organization, existing value can be protected and new value can be created. As organizations move through the ERM cycle, they should begin to demand more from their ERM investment. Accordingly, performance management, strategic management, and capital allocation decisions should systematically integrate consideration of risk.

When the value link is apparent, ERM will have begun to contribute more substantially to the competitive benefit of the enterprise.
Contacts

João Frade
Leader
Enterprise Risk Services
Deloitte & Associados, SROC S.A.
jfrade@deloitte.pt
+351 21 042 75 58

Alexandre Ferreira
Internal Audit
Enterprise Risk Services
Deloitte & Associados, SROC S.A.
alexferreira@deloitte.pt
+351 21 042 75 20