



2011 Enterprise Risk Management Survey

As originally published in the 2011 RIMS Benchmark Survey™





2011 Enterprise Risk Management Survey

Authored by

RIMS
1065 Avenue of the Americas, 13th Floor
New York, NY 10018
www.RIMS.org

Advisen Ltd.
1430 Broadway, 8th Floor
New York, NY 10018
www.advisen.com

Publishers

Mary Roth, ARM, RIMS
Thomas Ruggieri, Advisen Ltd.

Editor-in-Chief

David Bradford, Advisen

Contributing Editor

Carol Fox, ARM, RIMS



The RIMS Benchmark Survey on Enterprise Risk Management

“Everybody talks about the weather, but nobody does anything about it,” according to the famous quote attributed to Mark Twain. Until a few years ago, much of the same could be said about enterprise risk management (ERM). It was a popular topic for white papers and conferences, and its benefits were emphasized repeatedly by corporate governance oversight bodies, economic think tanks, rating agencies, and risk management experts, but few companies had made much progress in implementing ERM programs.

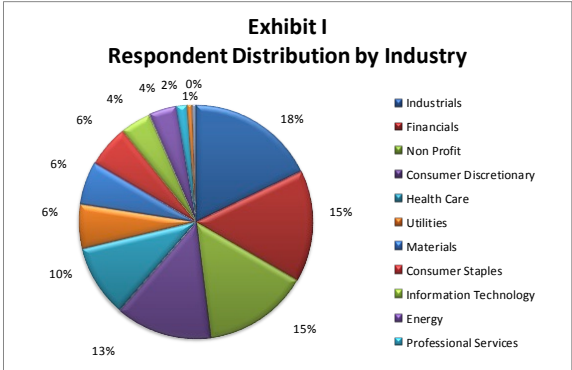
Based on the findings of this special RIMS ERM survey, conducted in conjunction with the *2011 RIMS Benchmark Survey™*, that state of affairs is quickly changing: more than half of the companies responding to the survey had partially or fully implemented an ERM program. This compares to 36 percent of companies responding to a similar survey just two years ago. Additionally, risk managers are much more frequently taking leadership roles in their company’s ERM programs: of companies with ERM programs, the risk management departments of nearly 60 percent of respondent companies were primarily responsible for driving ERM activities as compared to only 32 percent in the prior survey.

About the survey and the respondents

The RIMS ERM survey was administered by Advisen Ltd. The Survey, which included a separate section on broker compensation, was conducted online in November, 2010. Of the 14,250 risk managers invited to participate, 1,431 completed at least a portion of the combined surveys, for a response rate of 10 percent. Approximately 94 percent of respondents were from North America. When responses were received from more than one individual at a company, the most complete response was used and the others discarded.

Respondents represented a broad spectrum of industries. Industrials topped the list with 18 percent of the total, followed closely by financial (15

percent), nonprofit (15 percent) and consumer discretionary (13 percent) (Exhibit 1). Respondents also were widely-distributed by size, though weighted towards large companies: 15 percent have revenue of less than \$100 million, 35 percent are between \$100 million and \$1 billion, and 50 percent have greater than \$1 billion.



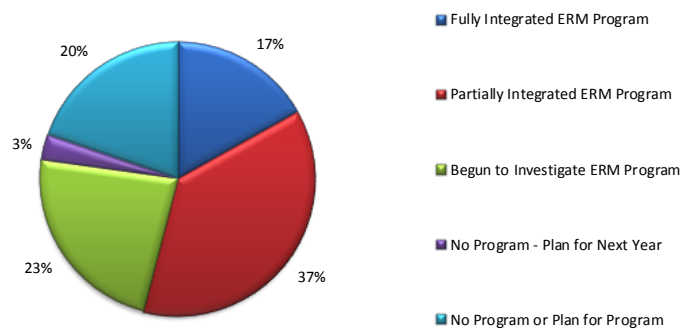
ERM adoption

In response to the question “To what extent has your organization adopted or is considering an enterprise risk management (ERM) program?” 17 percent said their organization has a fully integrated ERM program, and 37 percent said they have a partially integrated program.¹ The 54 percent of companies with partially or fully implemented ERM programs far exceeds the 36 percent of respondents answering the same question in 2008. Twenty-six percent are investigating or plan to embark on an ERM program in the next year. These responses suggest that enterprise risk management is becoming an accepted mainstream business discipline. Nevertheless, 20 percent said their company has no ERM program and has no plans to look into it (Exhibit 2).

¹ "Fully integrated ERM program" was described as "practiced at corporate level AND within EVERY operation/business unit and resource function." "Partially integrated ERM programs" was described as "practiced at corporate level OR at one or more operational / business unit or resource function levels."

These responses suggest that enterprise risk management is becoming an accepted mainstream business discipline.

Exhibit 2
Extent to Which ERM Program is Adopted



Large companies were far more likely than small companies to have a partially or fully integrated ERM program. Among the largest companies, those with revenues greater than \$10 billion, a whopping 85 percent reported having a partially or fully integrated ERM system, as compared to 39 percent of companies with revenue less than \$100 million.

ERM adoption rates varied materially by industry

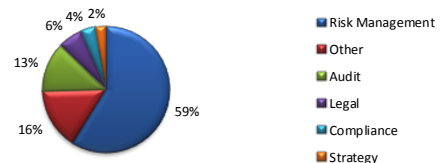
The industries with the highest percent of respondents representing companies with partially or fully implemented ERM systems were information technology (69 percent), energy (67 percent), financial (66 percent), and utilities (63 percent). The lowest adoption rates were in materials (43 percent), nonprofit (43 percent), telecommunication (43 percent), consumer discretionary (42 percent), and professional services (25 percent). While regulatory requirements may explain a portion of this variance, particularly for the financial sector, the industries represented by the highest adoption rates all – with the sole exception of telecommunications – are related to critical infrastructure where resiliency and sustainability are vital.

The risk manager’s role in ERM

Respondents to the 2009 survey reported that only 32 percent of ERM programs were led by the Risk

Management Department. By contrast, 59 percent of respondents to the current survey said the Risk Management Department leads the ERM program in their companies. The Audit Department came in at a distant second with 13 percent (Exhibit 3). A number of respondents choosing “Other” indicated in written responses that their organizations have dedicated enterprise risk management departments.

Exhibit 3
Department Primarily Responsible for Directing ERM



Smaller companies are most likely to have ERM programs led by risk managers. For companies with revenue less than \$500 million (15 percent of the respondents), ERM programs were led by the Risk Management Department in 71 percent of cases.

While the Risk Management Department often took a lead role in managing ERM programs, it was not the only department within a company to play a role.

In response to the question “Which risk functions within your organization are included in ERM activity planning and execution?” more than three-quarters of respondents said “Legal,” while 72 percent said “Audit” and two-thirds responded “Compliance.” Other high-ranking answers include “Strategic Planning” (63 percent),” Business Continuity” (62 percent),” Treasury” (58 percent) and “It Risk Management” (57 percent) (Exhibit 4). These responses emphasize the collaborative nature of the discipline and the necessity to include internal stakeholders and subject matter experts in ERM planning, as well as in execution.

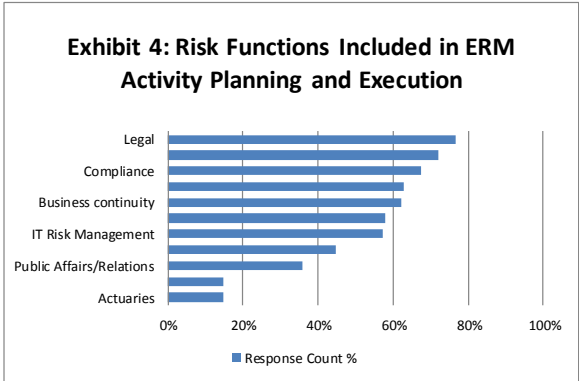
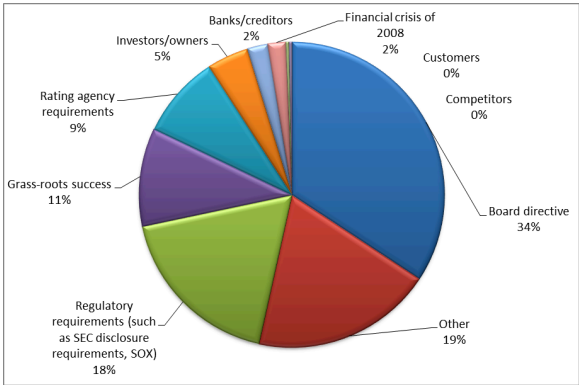


Exhibit 5: Principal Motivation for Implementation and/or Expansion of the ERM Program



ERM program drivers

An organization’s board of directors most often was the impetus for the creation of an ERM program.

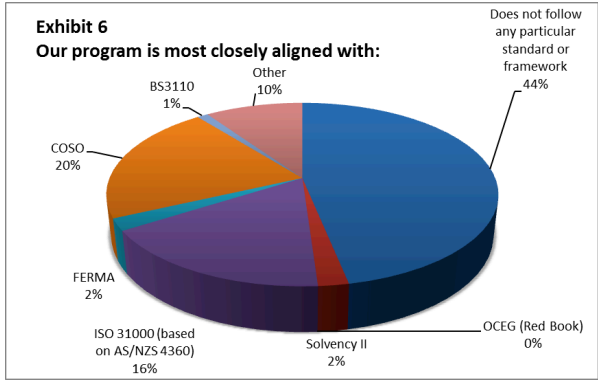
In response to “Was the implementation and/or expansion of the enterprise risk management

program primarily motivated by:” “Board directive” was chosen by about one third of respondents.

Eighteen percent of respondents chose “Regulatory requirements (such as SEC disclosure requirements, SOX)” “Grass roots success” was cited by 11 percent of respondents, and “Rating agency requirements” by 9 percent. Among those that chose “Other” (19 percent), some respondents wrote in that ERM was a C-level directive while a sizeable number of others said that it was a risk management department initiative (Exhibit 5). The responses were largely consistent by company size.

The board directive response may be driven by the governance drivers noted earlier, or it may be the viral-like outcome of board members serving on multiple boards. As the value of ERM as a business discipline is recognized in one organization, these practices are carried to other organizations on which the members serve.

A number of organizations have promulgated enterprise risk management frameworks, but none have proven to be especially influential with survey respondents (Exhibit 6). In response to “Our ERM program is most closely aligned with the following:” the most frequently chosen answer was “Does not follow any particular standard or framework,” accounting for 44 percent of respondents. This would suggest that organizations are either developing their ERM programs organically, or more likely are following productivity leader W. Edward Deming’s recommendation to “adapt, not adopt.”

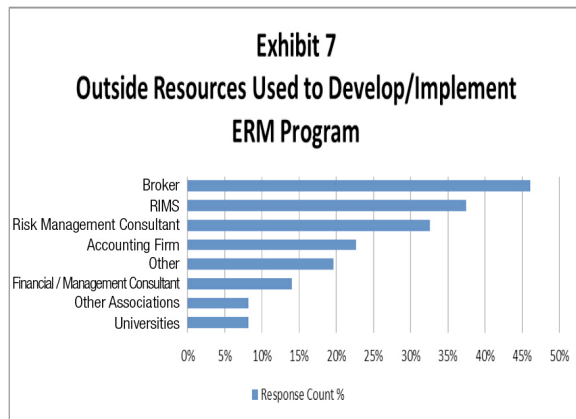


The most frequently chosen answer was: "Does not follow any particular standard or framework."

With respect to specific adopted frameworks, "COSO" (Committee of Sponsoring Organizations of the Treadway Commission) was selected by 20 percent of respondents. At 18 percent, ISO 31000 was the second most common standard. Other frameworks or standards chosen include Basel Accords, an international banking standard (6 percent), Solvency II, a European Union standard for insurance company solvency (2 percent), and BS31100, the British Standard Code of Practice for Risk Management (1 percent).

Developing and growing an ERM program

Survey participants were asked what resources they used, or are planning to use, to develop and implement their ERM programs. At 46 percent, "Broker" was the most common response, followed by RIMS (36 percent), and "Risk management consultant" (33 percent) (Exhibit 7). These responses admittedly may reflect a certain bias from the respondents based on the nature of the benchmark survey and its sponsors.

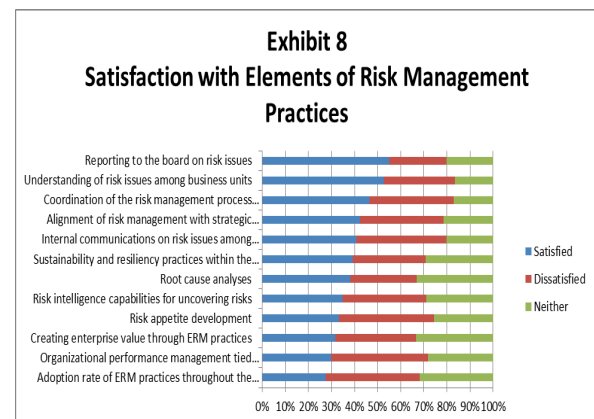


Asked whether their organizations had developed risk appetite and/or risk tolerance statements (one of seven success attributes highlighted in the RIMS Risk Maturity Model), 45 percent responded "No." Some of the remaining organizations apparently develop risk appetite or risk tolerance statements at

more than one level since 35 percent responded "Yes, Enterprise level," 25 percent said "Yes, Business unit or divisional level," and 15 percent said "Yes, Department level." These responses reflect the wide variety of risk appetite statements an organization may consider.

When asked about various elements of their organizations' risk management practices over the past year, survey participants were widely split among being "Satisfied," "Dissatisfied," and "Neither Satisfied or Dissatisfied." In total, for all the listed practices, 39 percent were "Satisfied," 35 percent were "Dissatisfied," and 25 percent were "Neither." The element with the highest degree of satisfaction is "Understanding of risk issues among business units," which was assigned "Satisfied" by 52 percent of respondents.

The elements with the lowest degree of satisfaction are "Organizational performance management tied to management's effectiveness in handling risk issues" (42 percent "Dissatisfied") and "Adoption rate of ERM practices throughout the organization" (41 percent dissatisfied) (Exhibit 8).



Value of ERM

Survey participants were divided in their perceptions of where ERM programs delivered the greatest value. In response to "The primary value we gain from our ERM program is..." nearly half (44 percent) of the respondents with ERM programs found the

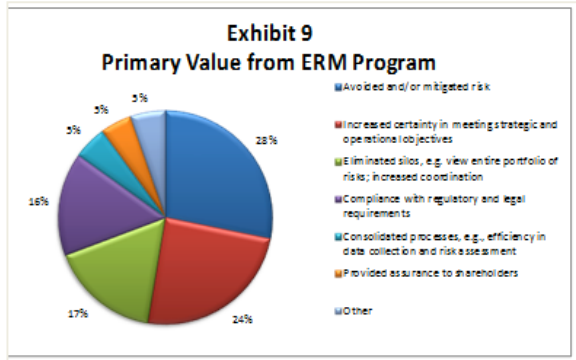
primary value to be in protection through risk mitigation (28 percent) and compliance (16 percent). This isn't terribly surprising as value protection is a comfort zone for most risk practitioners and reflects a historic board and management expectation. Arguably, value protection is important. However, it is difficult to articulate and demonstrate in terms of enterprise value just what the control framework produced in preventing a potential adverse event or mitigating the impact of an event or trend that didn't materialize.

Nearly half ... found the primary value to be in protection, while almost one quarter found it to be in increased certainty for achieving the organization's strategic and operational objectives.

Twenty-two percent added to their organizations' value through efficiencies gained by eliminating silos (17 percent) and consolidating processes within the ERM process itself (5 percent). These are important contributions but they may be viewed as holding relatively limited enterprise value when viewed in the context of the organization's overall objectives.

Only 24 percent found the primary value to be in increased certainty for achieving the organization's strategic and operational objectives. Remarkably, this would seem to be where risk management can add most to the organization's enterprise value.

The remainder cited providing assurance to shareholders (5 percent) and other value (5 percent) (Exhibit 9).



The perceived importance of ERM is attested to by the large numbers of senior managers who review ERM reports. Over half of respondents said that ERM reports/outputs are reviewed by the "Executive committee," while nearly half chose "CEO" and "Management risk committee." About one quarter chose "Another C-level executive." Only 5 percent said that no regular review process is in place.

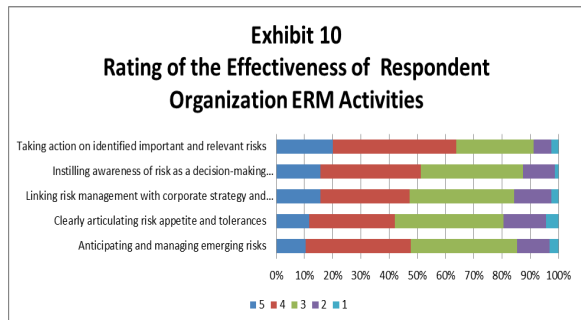
Scope and effectiveness of ERM

The enterprise-wide scope implicit in an ERM program has not been fully realized, in that only 17 percent responded that their programs are fully implemented (Exhibit 2). The scope of identified risks across the enterprise appeared to be more broadly developed. Given a list of typical risk categories, more than 90 percent of respondents said that their organizations evaluated nearly all of them. Ranking of the identified categories revealed the most commonly cited risk category evaluations:

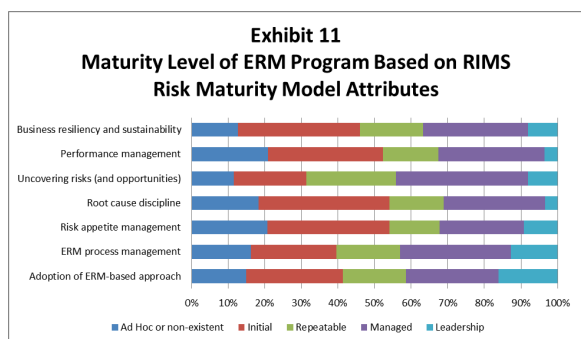
- Financial (97 percent)
- Operational (97 percent)
- Regulatory/Legal (95 percent)
- Compliance (94 percent)
- Information Technology (92 percent)
- Strategic (90 percent)
- Human Resources (87 percent)

Using a scale of 1=poor and 5=excellent to rate their ERM program activities, the results in Exhibit 10 (next page) indicate that respondents believe that they are most effective in taking action on identified important and relevant risks (>60% rating effectiveness as good to excellent), and instilling awareness of risks (>50% rating effectiveness as good to excellent). The areas noted as least effective are (a) in clearly articulating risk appetite and tolerances (nearly 60% rating effectiveness as poor to average), followed closely by (b) linking with corporate strategy and planning and (c) identifying new and emerging risks (each with >50% of the respondents rating effectiveness as poor to average).

Least effective ERM activity is in clearly articulating risk appetite and tolerances.



Based on the seven RIMS Risk Maturity Model attributes noted in Exhibit 11, very few respondents felt that their ERM programs had attained the highest level of maturity, “Leadership.” “Adoption of ERM-based approach” was the attribute receiving the highest “Leadership” ranking with 15 percent. “Performance management” had the lowest ranking, with only 3 percent claiming “Leadership” status and 31 percent claiming to be “Ad hoc or non-existent.” When asked which of the same attributes they wanted to see mature within their organizations to a higher level, 90 percent chose “Uncovering risks and opportunities,” 88 percent chose “Business resiliency and sustainability,” and 87 percent selected “Risk appetite management.”



Conclusions

The number of organizations with partially or fully implemented ERM programs has increased markedly since a similar survey was conducted two years ago. Additionally, risk managers are more often assuming leadership roles in ERM programs. The collaborative

approach among various risk functions is clearly valued in most organizations, with output from the ERM process reviewed by senior management. However, most organizations still have a distance to go before their ERM programs are fully optimized and generate strategic enterprise value by providing increased certainty for achieving the organization’s strategic and operational objectives.

Few respondents characterized their programs as fully mature. For three of seven RIMS Risk Maturity Model attributes, more than half of the respondents said their programs were at either the “Ad hoc or non-existent” or “Initial” stages. Furthermore, while most respondents believe that their organizations do a reasonably good job with respect to certain ERM-related functions, more than one-third were dissatisfied with various elements of their organizations’ risk management practices. Among the functions with the lowest level of satisfaction are “Organizational performance management tied to management’s effectiveness in handling risk issues” (42 percent dissatisfied), “risk appetite development” (41 percent dissatisfied), “Adoption rate of ERM practices throughout the organization” (40 percent dissatisfied), and “Internal communications on risk issues among risk functions” (39 percent dissatisfied).

In the 2009 survey, we concluded: “Despite obstacles, risk managers have the opportunity to expand their responsibilities and to take a much higher profile role in senior-level decision-making by championing ERM within their organizations.” While obstacles remain, many risk managers have seized the opportunity and have become ERM champions and risk leaders. Although many organizations are still at the earliest stages of ERM implementation, and other organizations struggle to fully implement efficient and effective ERM programs, it is clear that ERM, and the role of the risk manager, is increasingly a valued part of corporate culture and business practices.