

# RIMS 2013

ENTERPRISE RISK MANAGEMENT SURVEY



## 2013 RIMS Enterprise Risk Management (ERM) Survey

SPONSORED BY:



Administered by: Advisen Ltd.  
Sponsored by: Zurich  
Authored by: RIMS and Advisen Ltd.  
Publishers: *Mary Roth, ARM and Thomas Ruggieri*  
Co-Editors: *Josh Bradford, Advisen and Carol Fox, ARM, RIMS*

## About Advisen

Advisen generates, integrates, analyzes and communicates unbiased, real-time insights for the global community of commercial insurance professionals. As a single source solution, Advisen helps the industry to more productively drive mission-critical decisions about pricing, loss experience, underwriting, marketing, transacting or purchasing commercial insurance.

## About RIMS

As the preeminent organization dedicated to advancing the practice of risk management, RIMS, the Risk Management Society™, is a global not-for-profit organization representing more than 3,500 industrial, service, nonprofit, charitable and government entities throughout the world. Founded in 1950, RIMS brings networking, professional development and education opportunities to its membership of more than 11,000 risk management professionals located in more than 60 countries. For more information on RIMS, visit [www.RIMS.org](http://www.RIMS.org).

## About Zurich

Zurich is one of the world's leading insurance groups, and one of the few to operate on a global basis. Zurich's mission is to help their customers understand and protect themselves from risk. With about 60,000 employees serving customers in more than 170 countries, they aspire to become the best global insurer as measured by their shareholders, customers and employees. Zurich helps individuals, small- and medium-sized companies and global corporations around the world understand and protect themselves from risk by offering a wide range of insurance products, solutions and advisory services. They are very proud of their position as thought leader in Financial Lines.

### *Copyright*

*©2013 by RIMS and Advisen Ltd. All right reserved. Advisen Ltd. Is a registered trademark. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including: as a basis for an algorithm, photocopy, recording, or any other information storage, retrieval system, or for 3rd party benchmarking, without prior written permission*

## Executive Summary

The idea of enterprise risk management (ERM), or managing organizational decisions and activities through a strategic risk discipline across a full risk spectrum, has long held appeal for many organizations. In the past, however, turning the theory of ERM into a reality had proven challenging for many of those same organizations. Fully understanding the concept, communicating the benefits and justifying its costs were often cited as hindrances. Based on the findings of this study, however, what was once largely fodder for risk management consultants, economic think tanks and ratings agencies is now increasingly viewed as a necessary practice by much of the risk management community, executive management and regulatory agencies.

## About the Survey

The 2013 RIMS Enterprise Risk Management (ERM) Survey is a follow up to the 2009 and 2011 surveys on the same topic. The purpose of the survey is to gain insight into the current state of, and ongoing trends in, enterprise risk management. The survey was conducted online for nine days, beginning February 20, 2013 and ending February 28, 2013. Invitations to participate were distributed via email to 13,075 risk managers, insurance buyers and other risk professionals. The survey was completed at least in part by 1,095 respondents, for a response rate of 8 percent.

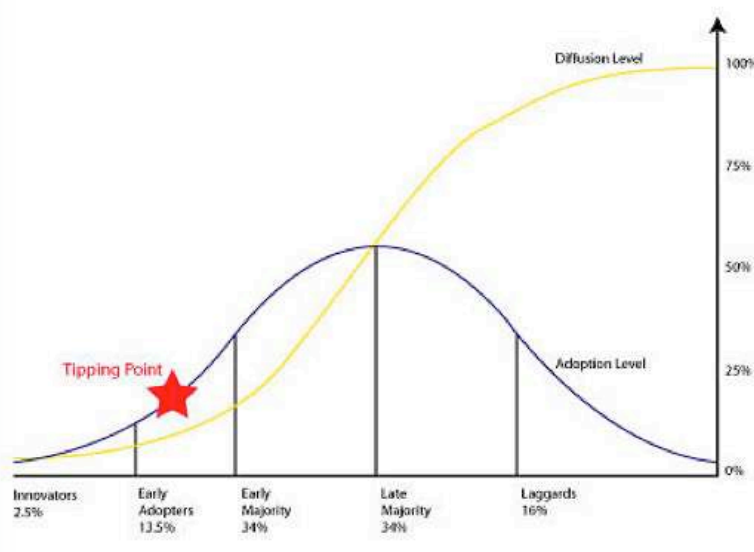
## ERM acceptance reaches critical mass

Results of the 2013 survey suggest that ERM, as noted in Everett Rogers' research on innovation diffusion and market acceptance, has now reached critical mass (over 60 percent). This is the point in time within the adoption curve that the sheer number of adopters assures that continued adoption of the innovation becomes self-sustaining and creates further growth (Exhibit 1). A tipping point occurs earlier, once an idea reaches a 15% to 18% adoption rate (beyond just the innovators and early adopters). In sociological terms, the tipping point is when a previously rare phenomenon becomes rapidly and dramatically more common. With successive groups of consumers adopting the new technology (shown in blue), critical mass pushes its market share (yellow) to eventually reach the saturation level.

In response to the question "To what extent has your organization adopted or is considering an enterprise risk management (ERM) program?" nearly 21 percent said they have a fully integrated ERM program to address risk, up 4 points from 2011 (when the tipping point first became evident for full integration). Forty-two percent said they have a partially integrated program, up 5 points from 2011. The combined 63 percent with either a partially or fully implemented ERM programs continues the upward trend in ERM adoption, from 54 percent in 2011 and 36 percent from 2009 (Exhibit 2).

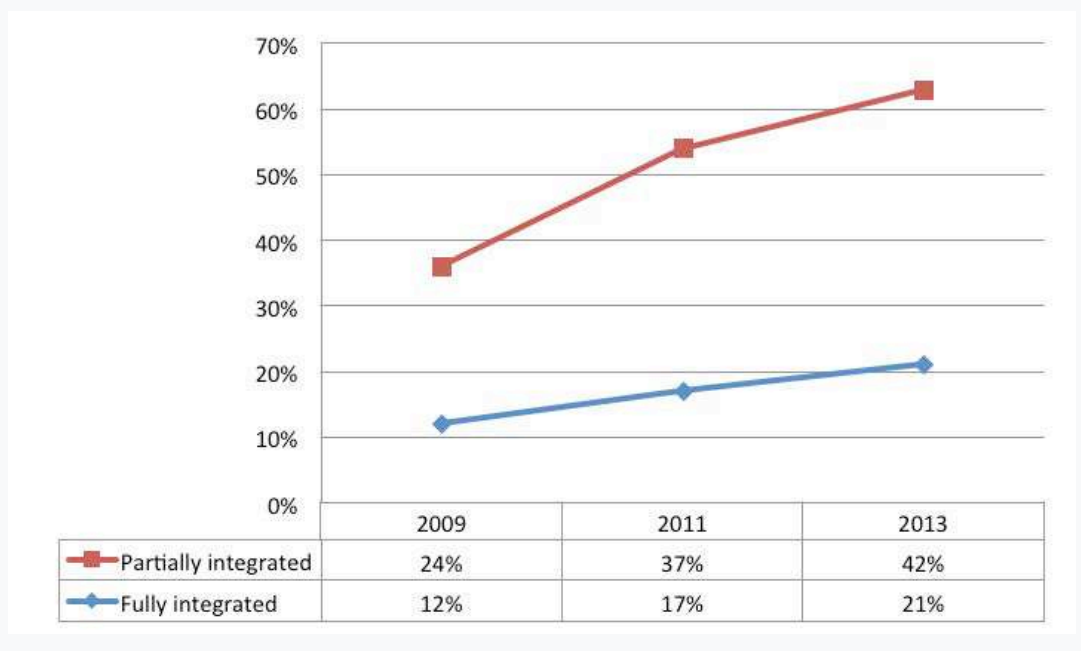
**Exhibit 1:** Rogers' Model: The diffusion of innovations according to Rogers (1962).

Source: Wikipedia



Of the respondents who do not have a full or partial ERM program, nearly 20 percent are either in the process or are planning to investigate an ERM program within the next year. This is down 6 points from 2011, explaining in part the increases in partial and full implementation. With 83 percent either adopting, in the process of adopting or considering adoption, this data also points to enterprise risk management continuing its upward trend as an accepted and mainstream discipline. Still, 17 percent of respondents do not have an ERM program (down 3 points from 2010). This suggests that a segment of the risk management community will be slower to – and in some cases may never – adopt the ERM discipline. This too is consistent with Rogers' theory that 16 percent lag in adoption.

**Exhibit 2: ERM Adoption Rates**

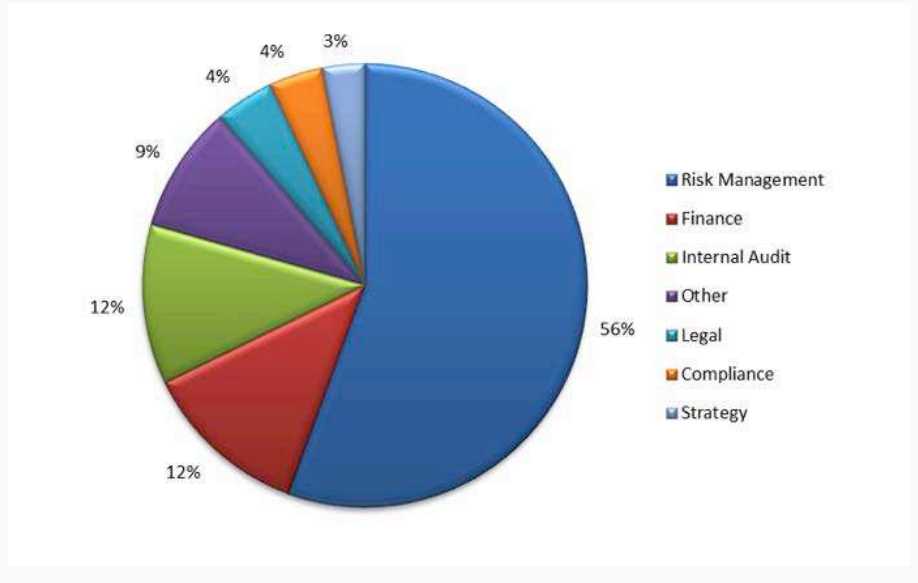


## The risk manager's role in ERM

Between the 2009 and 2011 survey there was a significant increase (27 points) in the risk management department's role in implementing ERM programs. Between 2011 and this year, however, the upward trend has leveled off. In response to the question "With respect to ERM in your organization, the department that is primarily responsible for directing ERM activities", 56 percent said risk management, down about 3 points from the 2011 survey. A new entrant this year, the Finance Department, came in second with 12 percent, along with Internal Audit also at 12 percent (Exhibit 3).<sup>2</sup> The emergence of Finance on equal footing with Internal Audit may signify greater alignment with organizational needs for risk impact analysis to include more detailed financial metrics, such as potential outcomes on capital, liquidity and earnings.

Even when the risk management department is not taking the lead role, risk management involvement in ERM activities is substantial. In response to the question "With respect to ERM in your organization, is the Risk Management Department involved with ERM activities?" only 3 percent said the department was not involved in ERM activities, and 68 percent reported full engagement.

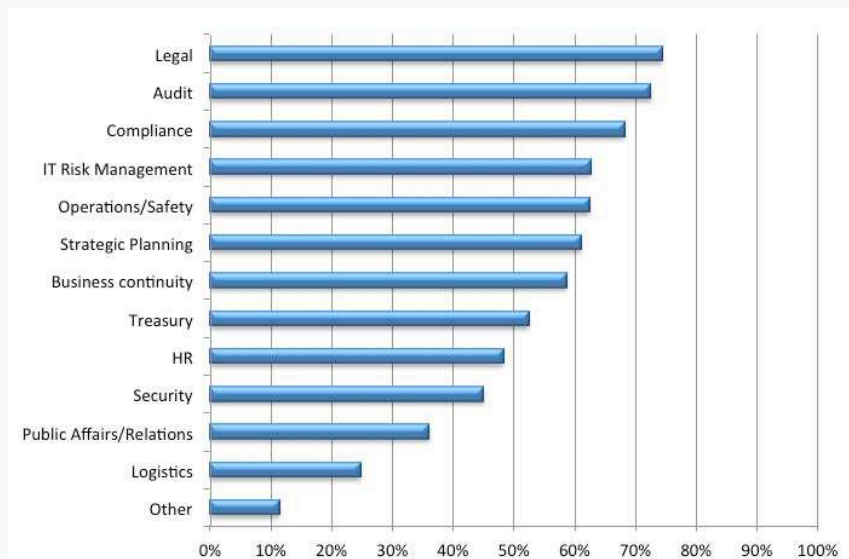
**Exhibit 3:** Department primarily responsible for directing ERM activities



While the Risk Management Department is heavily involved in the ERM program, many other departments within an organization also play active roles (Exhibit 4). We posed the question “Which risk functions within your organization are included in ERM activity planning and execution?” Consistent with the 2011 survey, three departments were named especially often: Legal (74 percent), Internal Audit (73 percent) and Compliance (68 percent). Other high ranking answers include IT Risk Management (63 percent), Operations/Safety (62 percent), Strategic Planning (61 percent) and Business Continuity (59 percent). All remained relatively consistent with the prior survey, with the exception of IT Risk Management which increased by six points from the previous survey. An emerging dependence on cloud technology for product and service delivery, along with frequent headlines about cyber threats, may have led to this area gaining prominence in ERM activities.

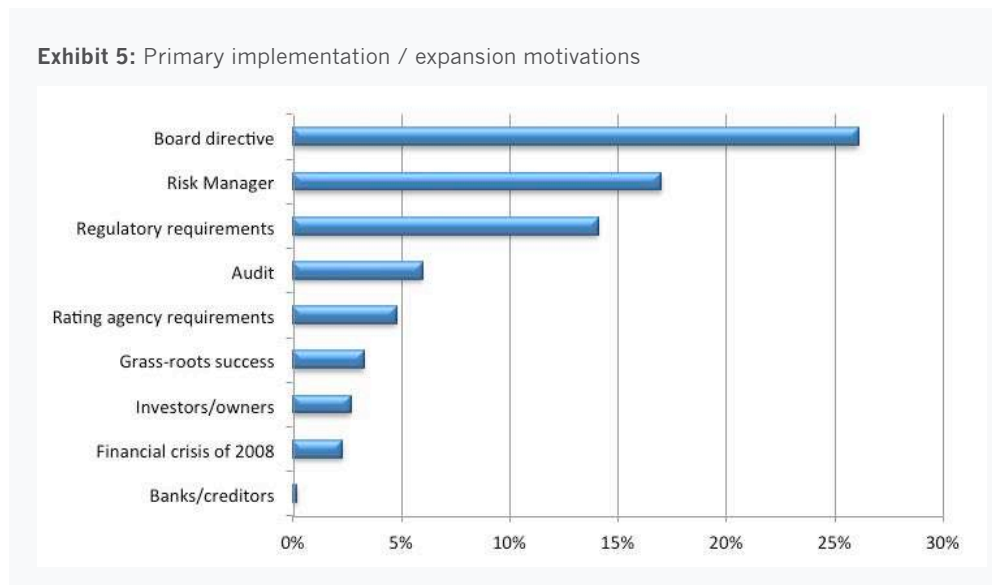
These responses continue to emphasize the collaborative nature of the discipline and the necessity to include internal stakeholders and subject matter experts in ERM planning, as well as execution. The fact that these percentages have remained relatively constant since 2011 – with one notable exception – signals an opportunity to engage the historically strongly linked areas more fully and encourage others, particularly those in treasury and human resources, to develop mutually beneficial plans.

**Exhibit 4:** Risk Functions Included in ERM Planning and Execution



## ERM Program Drivers

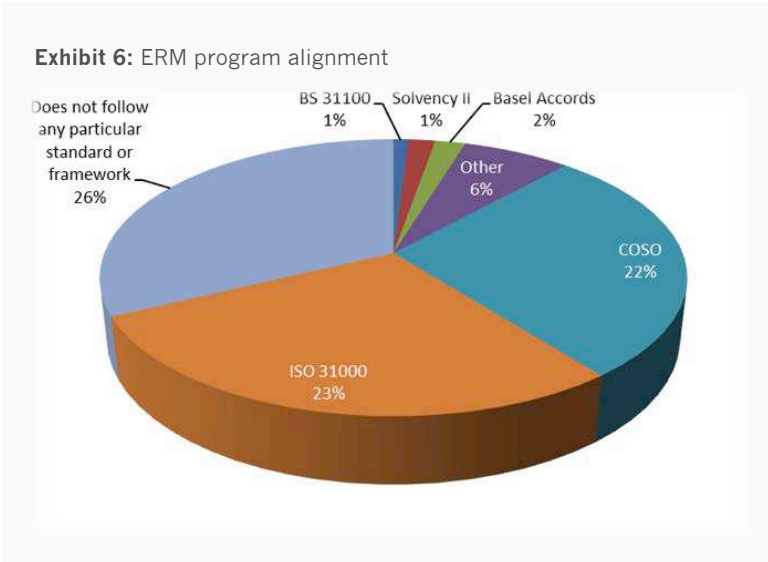
Board directive continued to be the most common driver of ERM programs but by less of a margin than in years past. In response to the question “Was the implementation and/or expansion of enterprise risk management program primarily motivated by”, “board directive” was chosen by 26 percent of respondents. This is down 8 percentage points from the 2011 survey. The second highest answer was “risk manager” at 17 percent, followed by “regulatory requirement” at 14 percent (dropping from 18 percent) and “other” at 12 percent. The “other” write-in responses varied but a significant percentage of respondents cited that ERM was an executive-level directive (Exhibit 5). Grass roots success and the impact of rating agencies as precipitating program drivers dropped significantly from 2011 (from 11 percent to 3 percent, and 9 percent to 5 percent, respectively).



“Risk Manager” was not a choice for this question in 2011 but was added to this year’s survey due to the high percentage of write-ins it received in the last survey. The fact that risk managers increasingly are the impetus of ERM programs should perhaps not be a surprise, based on the high percentage of risk management involvement previously discussed.

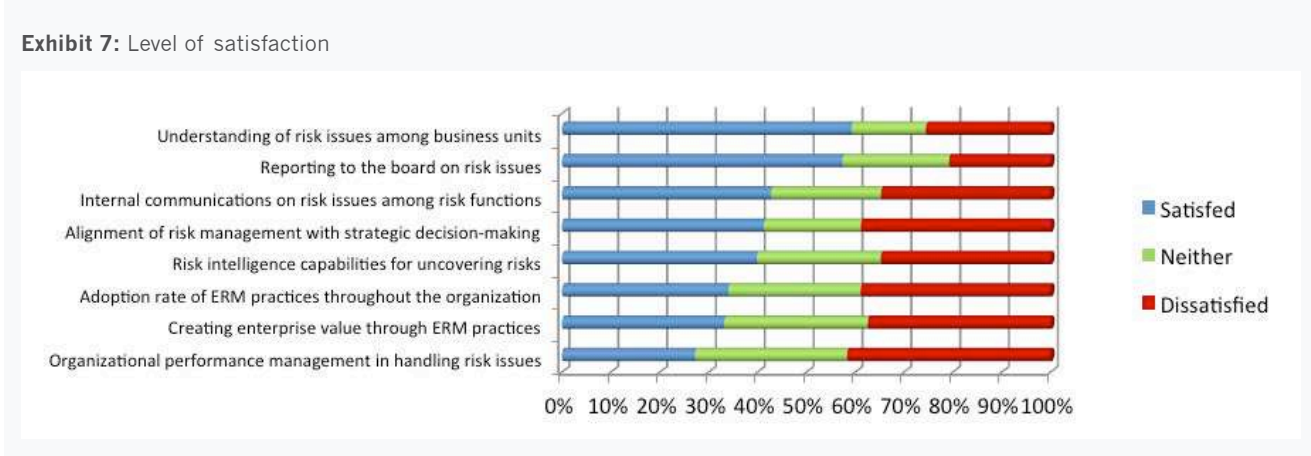
To some, ERM remains an abstract concept. A handful of organizations, however, have adopted or adapted ERM standards and frameworks in an attempt to formalize the discipline within their organizations. According to the results of this survey, more organizations are choosing to align their ERM programs with a specific standard or framework than in years past, as noted in the responses to “Our ERM program is most closely aligned with the following...” choices (Exhibit 6).

Growth in the use of the international ISO 31000 standard was the greatest, cited by 23 percent of respondents, a 5 percentage point increase from 2011. Second was the COSO ERM framework with 22 percent, a 2 percentage point increase from 2011. The most frequently chosen answer remained “Does not follow any particular standard or framework,” accounting for 26 percent of responses, with 19 percent indicating they “don’t know”. The remaining survey choices each garnered less than 2 percent of the respondents. Whether an organization chooses to adopt one of these standards or, as recommended by productivity leader W. Edward Deming, adapt the standards and practices that work best within their organizations, risk professionals need to be knowledgeable about these and emerging standards in order to remain relevant.



**Satisfaction with ERM**

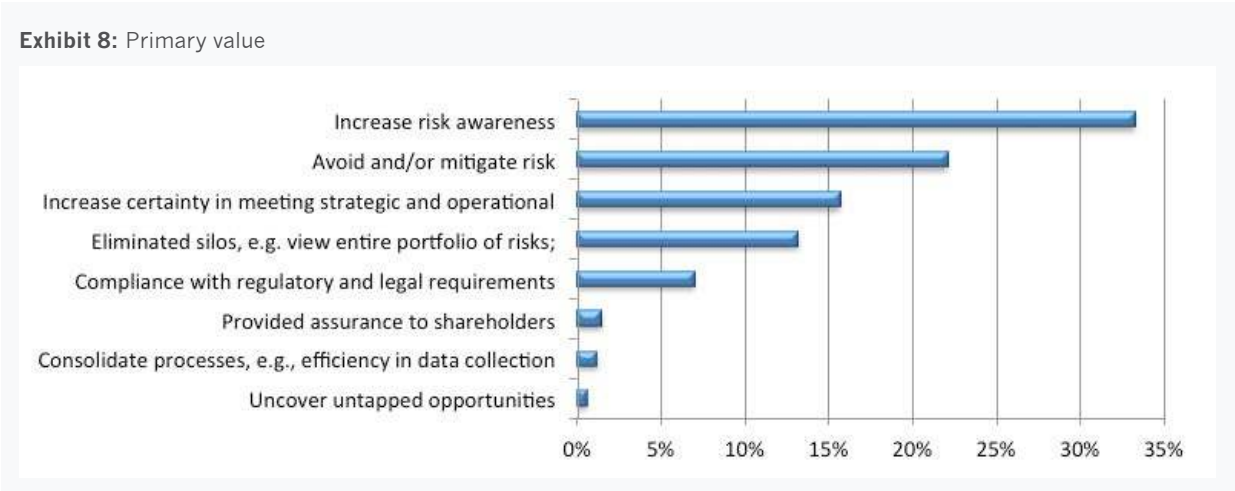
Participants were asked about their level of satisfaction with certain elements of their organization’s enterprise risk management practices. The element with the highest degree of satisfaction remained “Understanding of risk issues among business units,” which was assigned “Satisfied” by 59 percent of respondents, up notably from 52 percent in 2011. The elements with the lowest degree of satisfaction also remained essentially the same as in 2011 with “Organizational performance management tied to management’s effectiveness in handling risk issues” assigned “Dissatisfied” by 42 percent (42 percent in 2011) and “Adoption rate of ERM practices throughout the organization” assigned “Dissatisfied” by 39 percent (41 percent in 2011) (Exhibit 7).



Participants were asked “Have you developed risk appetite and/or risk tolerance statements<sup>3</sup> within your organization?” Consistent with the 2011 survey (45 percent), 48 percent said no. As in previous years, organizations that develop risk appetite or risk tolerance statements vary as regards the level of the organization at which these statements are developed: 34 percent responded “Yes, Enterprise level” (34 percent in 2011), 19 percent said “Yes, Business unit or divisional level” as compared to 25 percent in 2011. Ten percent said “Yes, Department level” as compared to 15 percent in 2011. Based on these results, organizations appear to be reducing the use of business and department level risk appetite and tolerance statements.

## The Value of ERM

When asked about the value their organization gains from an ERM program, a third of the respondents found the primary value to be increasing risk awareness, followed by avoiding and/or mitigating risk (22 percent), increased certainty in meeting strategic and operational objectives (16 percent) and eliminating silos, e.g. view entire portfolio of risk; and increased coordination (13 percent each) (Exhibit 8). These results may reflect an increased interest in ERM activities by executive management, including the board of directors, to obtain a more holistic view of organizational risk.



## ERM Expectations and Effectiveness

In this year's survey, we focused on executive management's expectations of the ERM Program (Exhibit 9) in order to compare how effective respondents believe their programs are in relation to these expectations. We asked respondents to indicate the top three expectations in order of importance (1 being most important). "Providing reasonable assurance that risks are managed" was ranked the top expectation, followed by "aligning risk appetite and strategic risks" and "improved certainty." Two others ranked high when combining primary and secondary expectations: "minimizing operational surprises and reducing losses" and "providing verifiable financial savings and cost avoidance."

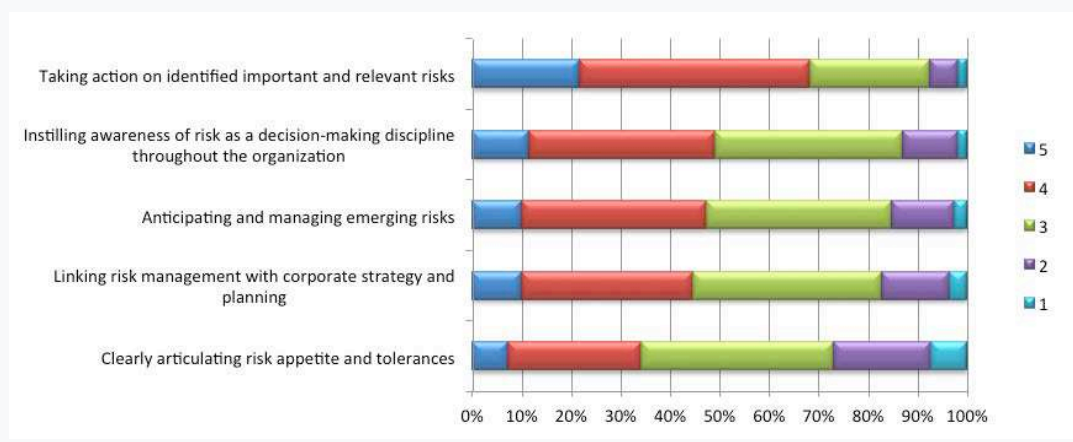




Using a scale of “1 = is not effective at all” and “5 = is highly effective” to rate their ERM program activities, survey participants were asked to rate the effectiveness of their organizations in various ERM categories. The results in Exhibit 10 indicate that nearly 70 percent of respondents believe that they are most effective in taking action on identified important and relevant risks, which aligns well with executive management’s expectations for assurance that risks are being managed. Nearly 50 percent noted that they were very or highly effective in instilling awareness of risk as a decision-making discipline, which also aligns well with executive management’s expectations.

The results also revealed a clear opportunity for improvement when it comes to executive management’s expectations for aligning risk appetite and strategic risk. Nearly 20 percent of the respondents noted that they were least effective or not effective at all in linking risk management with corporate strategy and planning, with only 10 percent indicating that they are very effective in this area. Additionally, over 25 percent noted that they were least effective or not effective at all in clearly articulating risk appetite and tolerances, with less than 10 percent indicating that they are very effective in this area.

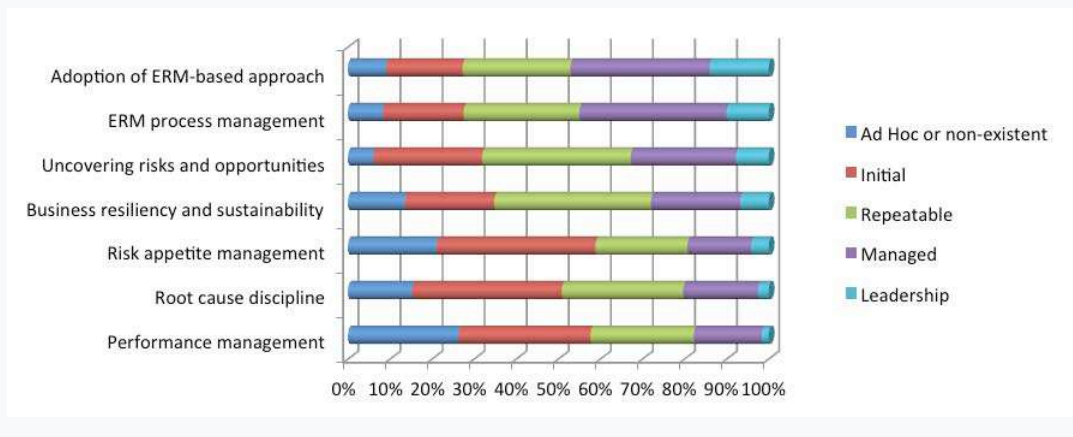
**Exhibit 10: ERM effectiveness**



## Perceived Maturity of ERM Program

Based on the seven RIMS Risk Maturity Model attributes noted in Exhibit 11, survey participants were asked to rate the maturity of their ERM programs, from ad hoc to a leadership level. The results remained relatively consistent when compared to the 2011 survey results. Very few respondents believe that their ERM programs have attained the highest maturity level (leadership) in any category. Adoption of ERM-based approach again was the attribute mostly consistently rated at the leadership level, with 14 percent claiming this achievement. Performance Management remained the most immature attribute with only 2 percent claiming leadership status and 26 percent claiming to be “ad hoc or non-existent.” When asked which of the same attributes they wanted to see mature to a higher level, 89 percent chose Risk Appetite Management, while 86 percent chose Uncovering Risks and Opportunities and Root Cause Discipline equally as needing more mature practices within their organizations. These results are based on perceptions. Risk professionals and internal auditors will want to compare these perceptions with the maturity of their own programs and practices by taking the RIMS Risk Maturity Model free self-assessment (available on RIMS website).

**Exhibit 11: Perceived Maturity of ERM Program**

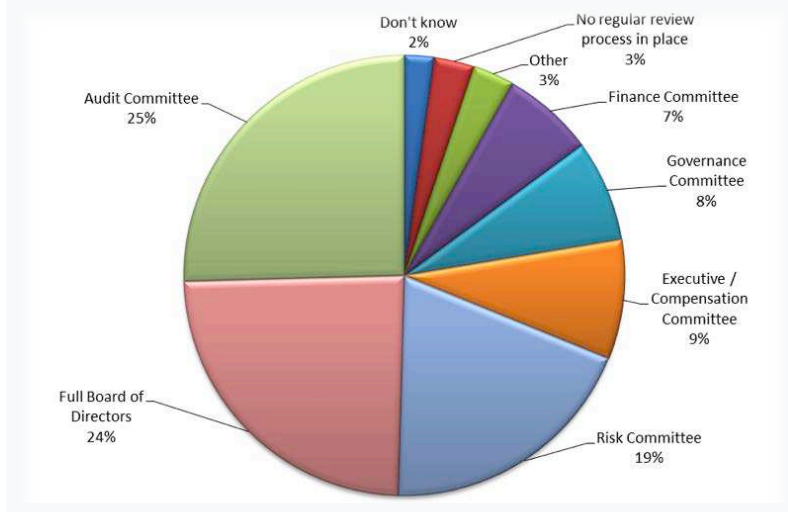


## Risk Reporting

In the 2013 survey, we asked about risk reporting practices, both at the board and executive level. As shown in Exhibit 12, results were split fairly evenly at the board level between the full board (24 percent) and the audit committee (25 percent), followed by a separate risk committee (19 percent), with the remainder split among other board committees (each less than 10 percent). Only 3 percent reported that no regular board review process is in place.

These results appear to confirm that risk reporting is being expanded to either the full board or a separate risk committee, rather than to the Audit Committee as has been historic practice.

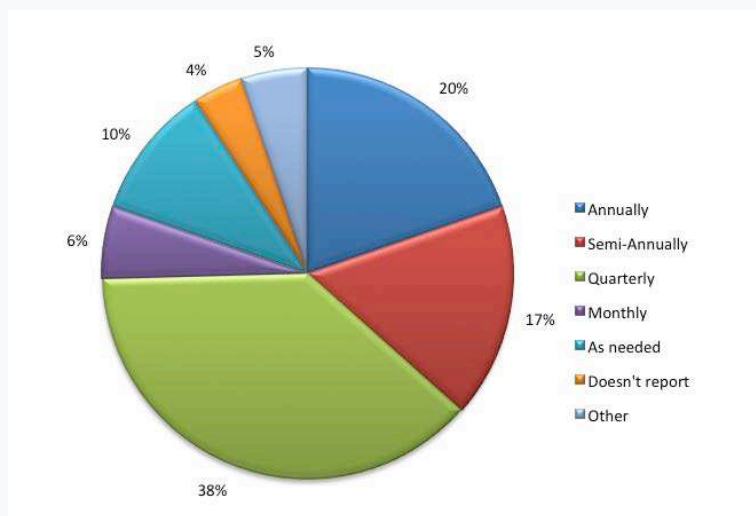
**Exhibit 12: ERM reports/outputs are reviewed at the board level by**



## Board Reporting Frequency

When asked how often the top risk executive reports to the board (Exhibit 13), 38 percent responded that reports were made to the board quarterly, 20 percent annually and 17 percent semi-annually. Six percent reported on risks monthly, with 10 percent reporting "as needed". Only 4 percent of the respondents indicated that the top risk executive did not report to the board or one of its committees.

**Exhibit 13: Board Reporting Frequency**



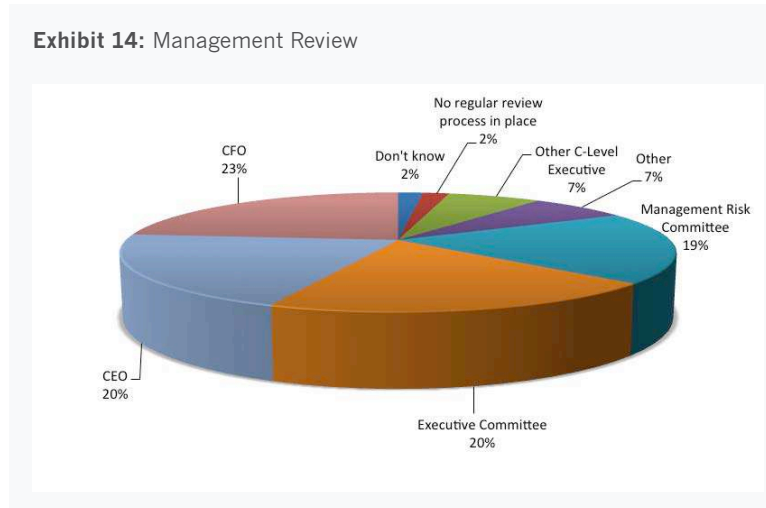
While nearly 45 percent of the total respondents indicated reports most often are made “quarterly or more frequently”, we noted a difference in reporting frequency depending on which board committee is responsible for risk oversight (Table 1). Perhaps not surprisingly, when a separate board risk committee has oversight, reports most often are made “quarterly or more frequently”, as indicated by 58 percent of the respondents with risk committees. Interestingly, reports more often are made “quarterly or more frequently” when the full executive/compensation committees or full boards have risk oversight responsibilities (55 percent and 52 percent respectively), while reports to audit committees are equally balanced in frequency between “annually or semi-annually” and “quarterly or more frequently”. When no regular review process is in place, reports generally are not made (41 percent) or only made as needed (28 percent). The increased reporting frequency when the full board, risk committee or executive/compensation committee has risk oversight may be indicative of a higher significance given to risk management within these organizations.

**Table 1. Board Reporting Frequency by Risk Oversight**

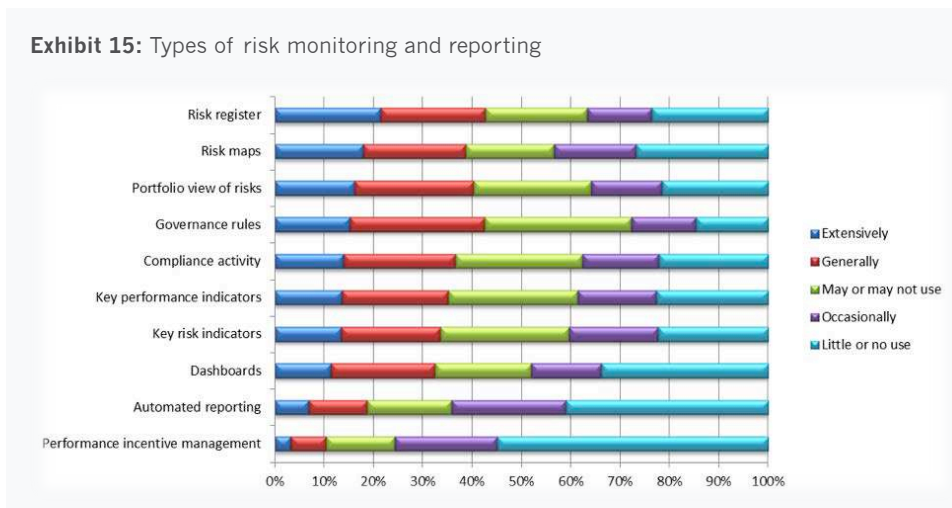
Risk Oversight	Annually or Semi-Annually	Quarterly or More Frequently	As needed	Does not report
Risk Committee	32%	58%	10%	0%
Executive/Compensation Committee	37%	55%	8%	0%
Full Board of Directors	40%	52%	6%	1%
Audit Committee	46%	46%	6%	2%
Finance Committee	42%	46%	9%	3%
Governance Committee	47%	42%	9%	1%
No regular review process in place	21%	10%	28%	41%

## Management Review

When asked about reporting to the executive level on ERM outputs (Exhibit 14), 23 percent of the respondents indicate that the CFO is the primary reviewer, followed closely by the CEO and Executive Committee at 20 percent each, along with a Management Risk Committee review at 19 percent. Only 2 percent indicated there was no regular review process in place at the executive level. This rather even distribution indicates that there is no consensus around which executive or committee has primary responsibility for reviewing ERM outputs and reports; organizations appear to be choosing what works best for their purposes.



When asked about the types of reports and tools that are being used for monitoring and reporting purposes (on a scale of 1 to 5 with 5 being extensively and 1 being little or no use), over 20 percent of the respondents indicated that risk registers are used extensively (Exhibit 15). Slightly fewer indicated extensive use of risk maps and portfolio views. Over 40 percent indicated that risk registers along with governance rules (that is, reporting tied to risk objectives) are extensively or generally used. Dashboards, automated reporting and performance incentive management reports and tools are least used.



As boards and executive management require more informed analyses, an opportunity exists for using reporting forms in addition to risk registers, such as key performance and risk indicators, more extensively. These types of reports tend to more closely align risk appetite and strategic risk, one of the key executive management expectations noted earlier in the report. Dashboards provide an opportunity to convey information and trending in a succinct and easily understandable way, without reams of data.

## Conclusion

In the 2011 survey, we concluded: "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." In 2013, we find that ERM indeed has reached "critical mass" as a management discipline with more than 60 percent of the respondents having fully or partially implemented ERM programs. Risk managers act as motivators and, by a wide margin, continue to take primary responsibility for directing ERM activities, with 97 percent engaged in ERM activities in some way. Of note is the emergence of the Finance Department as an ERM leader, potentially signifying a demand for risk impact analyses to include more detailed financial metrics, such as risk outcomes on capital, liquidity and earnings.

Many other departments play active roles in ERM planning and execution, most notably legal, internal audit and compliance, and increasingly IT Risk Management. Nevertheless, the 2013 survey results signal an opportunity to engage these as well as other functions, such as strategic planning, operations, business continuity, treasury and human resources, in a concerted way. More organizations are choosing to align their ERM programs with a specific standard or framework, with notable growth in the use of the international ISO 31000 standard, although more than a quarter of the respondents indicate that they do not follow any particular standard or framework. This may be an opportunity to adopt - or adapt - published practices in ways to advance risk management to further organizational goals and objectives.

The primary cited value that organizations gain from ERM programs is increasing risk awareness, followed by avoiding and/or mitigating risk and increasing certainty in meeting strategic and organizational objectives. While nearly 60 percent of the respondents are satisfied both with the understanding of risk issues among business units and how they are reporting to the board on risk issues, over 40 percent are dissatisfied with ERM's alignment with strategic decision-making and organizational performance management in handling risk issues. In comparing what the respondents reported as executive management's primary expectations of the ERM program with the effectiveness of the ERM program, we found both alignment and potential misalignment. Nearly 70 percent of respondents believe that they are most effective in taking action on identified important and relevant risks and 50 percent noted that they are very or highly effective in instilling awareness of risk as a decision-making discipline. Both align well with executive management's expectations for assurance that risks are being managed. On the other hand, executive management's expectations for aligning risk appetite and strategic risk may not be fully lined up, which presents a significant opportunity for improvement. Twenty percent report that they are least effective or not at all effective in linking risk management with corporate strategy and planning. Additionally, over 25 percent noted that they are least effective or not effective at all in clearly articulating risk appetite and tolerances. Only ten percent or less indicated that they are highly effective in these two areas.

Again this year, few respondents characterized their programs as fully mature. For example, nearly 60 percent said their programs are ad hoc or in the initial stages in the risk appetite management and performance management attributes. More than 40 percent expressed dissatisfaction, primarily with three elements of their organizations' risk management practices. Among the practices with the lowest levels of satisfaction are 1) organizational performance management tied to management's effectiveness in handling risk issues, 2) adoption rate of ERM practices throughout the organization, and 3) alignment of risk management with strategic decision-making.

In this year's survey, we asked about risk reporting practices, both at the board and executive level. The results seem to confirm that board risk reporting is occurring more often at the full board (24 percent) or to a separate board-level risk committee (19 percent) than in the past, when the Audit Committee held primary responsibility for risk management oversight. That said, 25 percent indicate that the top risk executive indeed is reporting to the Audit Committee. Board reporting frequency is conducted most often on a quarterly basis (38 percent). Another 37 percent report to the board either annually (20 percent) or semi-annually (17 percent). Board reporting frequency appears to increase when risk oversight responsibility falls to a separate board risk committee, the executive/compensation committee or the full board of directors, with more than 50 percent reporting quarterly or more frequently. ERM reports to management are generally reviewed by the CFO, CEO, Executive Committee or a Management Risk Committee. Risk registers are used extensively by more than 20 percent of the respondents; slightly fewer use risk maps and portfolio views extensively. As boards and executive management require more informed analyses, an opportunity exists for using reporting forms – such as dashboards with key performance and risk indicators - that more closely align risk appetite and strategic risk in order to meet expectations.

This year, we would like to conclude with an observation, a warning and a challenge. The observation: we risk professionals now have what we wished for – risk management, particularly enterprise risk management, is now recognized by a majority of organizations as a strategic business discipline across the full risk spectrum. Furthermore, it is considered a valued part of corporate culture and business practices at the board and executive levels. As risk professionals, we can be pleased with this progress. The warning: this survey revealed a number of misalignments between risk management effectiveness and executive management expectations. We can use these results to examine our own programs, and recommit in delivering the expected value to our organizations. The challenge: the task of maturing risk practices to create value - as well as protect it - is not for the faint of heart. Often described as a journey, fully integrating ERM can be arduous. The good news is that the result is well worth the effort, as many organizations have already discovered.

NOTES:

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

<sup>2</sup> 1 percent of the total respondents (identified by written response in the "other" answer option) indicated that their organization has a dedicated enterprise risk management department.

<sup>3</sup> Risk appetite and/or risk tolerance statements: one of seven success attributes highlighted in the RIMS Risk Maturity Model