RESEARCH REPORT

October 2015

Mastering Risk

The State of Risk Management in Canada 2015

A Survey Report by Jim Barbour, CPA, CIA, Jonathan Burnett, ACA,
Sheila Smigarowski, CA, CIA, CRMA, and R. Michael Varney, CPA, CIA

Crowe Horwath®

The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

In early 2015, Crowe Risk Consulting, in collaboration with the Institute of Internal Auditors (IIA) Canada, launched an inaugural survey of risk management professionals to identify best practices in internal audit and risk management in Canadian organizations. This survey was undertaken as part of an ongoing initiative to recognize organizations that have demonstrated sustained efforts toward mastering risk. This report examines the survey responses and explores the implications of the survey findings. During the course of this analysis, four major themes emerged. These themes suggest areas in which organizations can find opportunities for improvement: first, by clarifying their approach to the three lines of defence model; second, by taking a more strategic approach that elevates risk management to a higher priority; third, by developing methods for demonstrating results; and fourth, by working with the audit committee and senior management to establish a "mastering risk" culture.

Table of Contents

Executive Summary: Assessing the State of the Profession 3

Improvement Opportunity 1:
Clarifying and Coordinating the Three Lines of Defence 6

Improvement Opportunity 2:
Taking a More Strategic Approach to Risk Management................. 10

Improvement Opportunity 3:
Demonstrating Results and a Positive ROI 14

Improvement Opportunity 4:
The Board and Senior Management as Risk Culture Champions.... 16

Conclusion: Responsibilities and Tools
for Establishing a Mastering Risk Culture 18

Unless otherwise indicated, the source of the exhibits throughout is Crowe Risk Consulting analysis. Due to rounding, the numbers may not sum to 100 percent.

Acknowledgments

We thank the following people for their assistance with this report. Special thanks go to the Conference Board of Canada's Strategic Risk Council for survey promotion.

IIA Canada Steering Committee
Richard Arthurs, AltaLink
John Fraser, Hydro One (retired)
Chandrasekhar Krishnamurthy, Hydro Ottawa
Jade Lee, AltaLink
Sheila Smigarowski

Project Team
Trevor Anderson, Jim Barbour, Chantal Gabriele, Carla Jillson, Andy McDaniel, R. Michael Varney, Kathy Willhoite, Andrea Wilton
– Crowe Risk Consulting
Judy Burke, Michael Eastman, Shannon Rose, Shelley Pelkey – IIA Canada

Executive Summary: Assessing the State of the Profession

Managing risk has been a fundamental concern in business and public organizations throughout history – even long before risk management was recognized as a distinct business discipline. In recent years, the focus on risk has intensified, as both private companies and public sector organizations seek ways to better organize and delegate responsibilities for managing risk and to develop more integrated and coordinated responses to risk – in essence, the need to master risk to gain competitive advantage.

Among the factors currently driving these efforts are intense regulatory pressure; the continued extension, via third parties, and expansion of enterprises; heightened concerns about data privacy; growing geopolitical risks associated with global enterprises; and nearly instantaneous communication capabilities that not only alter behaviour but also create new categories of risk.

In the face of these growing pressures, and in light of global studies about how the practice of risk management is evolving elsewhere, Crowe Risk Consulting and the Institute of Internal Auditors Canada (IIA Canada) launched an inaugural survey to examine the state of Mastering Risk in Canada. Those surveyed were risk management professionals who were engaged in various aspects of risk management as their primary areas of responsibility – that is, they were members of the internal audit, risk management, or internal control functions, along with operational managers who have responsibility for the application and maintenance of internal controls.

While board members and audit committee members did not participate in the survey, it could be argued that in some ways they should have the most direct interest in the survey results. The participants were those people who must ultimately answer to the board, and in many cases interact directly with the audit committee. The observations of risk professionals on the front line can provide board members with valuable perspectives into ways that the board's participation can help strengthen their organizations.

The main survey questions covered two broad categories of information:

- Organization of the risk management functions (internal audit, risk management, and internal control)
- Specific risk management framework and practices within the organization

The responses to the survey questions provide useful insights into the state of mastering risk in Canada today. More important, a review and analysis of these responses can provide guidance into how Canadian businesses and public sector organizations might improve the effectiveness of their efforts.

About the Survey

The survey questions were distributed online by Crowe Risk Consulting, in collaboration with IIA Canada. The survey, promoted to the membership of IIA Canada through various types of media, was conducted from February 2015 to April 2015 using an online survey software application that led participants through a series of interactive questions about risk management responsibilities (internal control, risk management, and internal audit) and specific practices in their organizations. More than 300 participants logged into the survey and responded to at least one of the questions; ultimately, 114 respondents completed the survey.

Exhibit 1: Survey Respondents by Industry

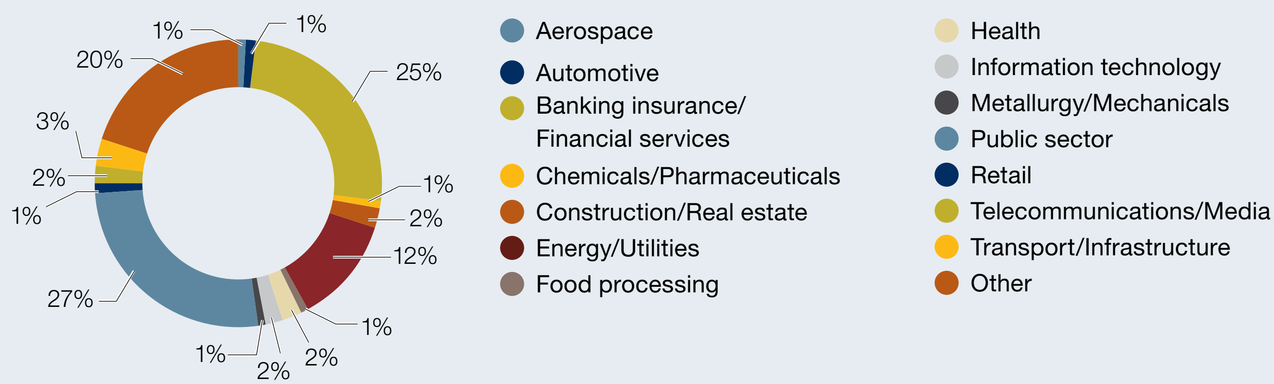
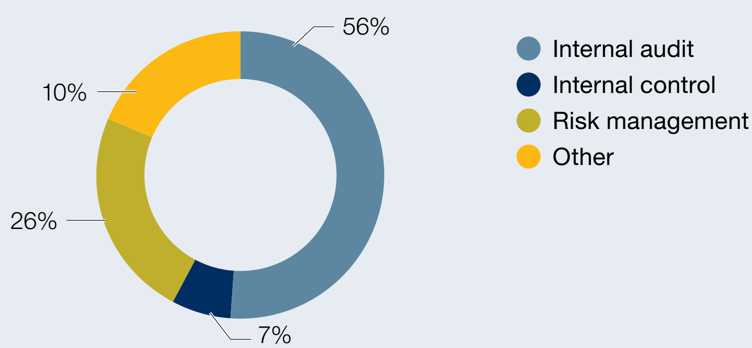


Exhibit 2: Survey Respondents by Position



The respondents represent a broad cross-section of Canadian industries and organizations, with heavy representation from the public sector and the banking, insurance, and financial services industries (Exhibit 1). More than half the participants said that they were part of their organization's internal audit function and more than a quarter reported being part of the risk management function. The remaining respondents held positions in internal control or other executive or administrative functions (Exhibit 2).

Four major opportunities for improvement emerged from the survey analysis:

1. **Applying and refining the three lines of defence model.** Although the three lines of defence model (management controls, risk management and/or compliance, and internal audit) is used widely, the roles and responsibilities associated with each function are often unclear or misunderstood. Improving coordination among these functions without blurring the lines between their distinct responsibilities can require a delicate balance and clear communication.
2. **Taking a strategic approach.** Survey responses indicate that people with major risk management responsibilities in their organizations often spend the majority of their time and effort focusing on tactical issues and the day-to-day operation and supervision of risk management functions. Much less attention is given to strategic-level decisions, such as identifying and assessing new areas of risk. The audit committee has a major role to play in elevating the risk management focus and creating a larger role for risk management and assurance in strategic decision-making.
3. **Developing methods for demonstrating results.** It can be particularly difficult to calculate and verify the financial value that risk management and assurance activities add to an organization, but demonstrating a positive return on investment (ROI) is essential to securing a greater commitment of time and resources to these functions. In short, the investments made in mastering risk must be seen as contributors to success – not just a cost of compliance.
4. **Working with the audit committee and senior management to establish a "mastering risk" culture.** The maturity of the risk management framework can be greatly enhanced by improving the quality of information provided to the audit committee, broadening the committee's focus beyond the finance and accounting disciplines, and including risk culture on the audit committee agenda.

This report explores these four themes, along with some of the specific survey responses that led to them. We conclude with some suggested areas of focus that could help management, audit committees, and other risk stakeholders address these concerns. We invite you to evaluate the survey findings in light of the four themes addressed here and to contact the authors with any questions, comments, or reactions as you hone your approaches to mastering risk.

Interested readers can read the complete, question-by-question report on all the survey results and a listing of all the questions and responses.

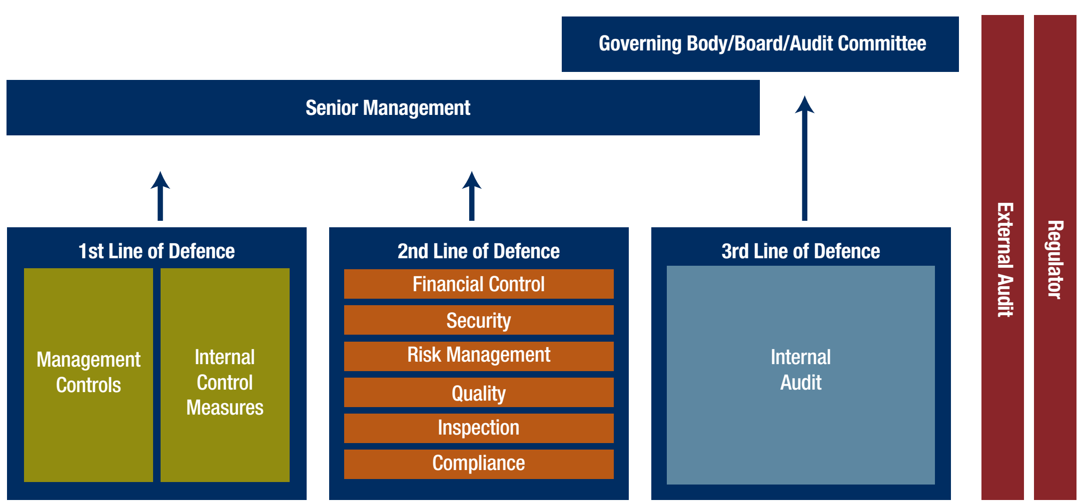
Improvement Opportunity 1: Clarifying and Coordinating the Three Lines of Defence

Over the years, the three lines of defence model has emerged as the de facto standard in financial institutions and is becoming more common for organizing and delegating risk framework and assurance responsibilities among the various management functions. A recent IIA position paper describes the model as an "effective way to enhance communications on risk management and control by clarifying essential roles and duties."[1] The paper's definition of the three lines of defence can be summarized as follows:

- First line of defence: Operational managers who own and manage risks. They also are responsible for maintaining effective internal controls, executing risk and control procedures on a day-to-day basis, and implementing corrective actions to address process and control deficiencies.
- Second line of defence: Risk management and compliance functions that help support and monitor the first line-of-defence controls. These functions facilitate and monitor risk management practices, provide risk management frameworks, identify known and emerging issues, assist risk owners in defining target risk exposures, and report risk-related information throughout the organization.
- Third line of defence: Internal audit, which provides the governing body and senior management with comprehensive, independent, and objective assurance on the effectiveness of governance, risk management, and internal controls. Its scope typically covers a broad range of objectives, including efficiency and effectiveness of operations; safeguarding of assets; reliability and integrity of reporting processes; and compliance with laws, regulations, policies, procedures, and contracts.

The IIA position paper illustrates the relationships among the various functions, as shown in Exhibit 3.

Exhibit 3: Three Lines of Defence Model



Adapted from the IIA position paper "The Three Lines of Defense in Effective Risk Management and Control," January 2013

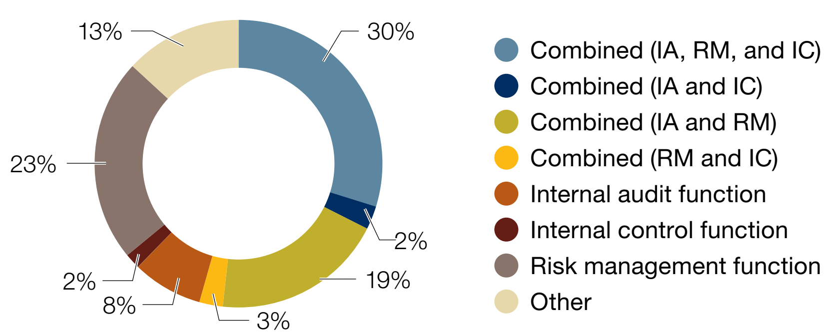
Most widely used risk management frameworks, such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management – Integrated Framework or the International Organization for Standardization's ISO 31000 risk standards, are compatible with this model and accommodate it, in practice, in their application. A 2015 research paper published jointly by The IIA and COSO builds on this model and notes, "When an organization has properly structured the three lines, and they operate effectively, there should be no gaps in coverage, no unnecessary duplication of effort, and risk and control has a higher probability of being effectively managed."[2]

Having no gaps in coverage and no unnecessary duplication of effort is a lofty goal, especially given the common tendency to merge the activities of these three functions (internal control, risk management, and internal audit) into one or two groups. That tendency is reflected in the survey responses. When asked to describe the organization of risk management functions, more than half (54 percent) of the respondents said at least some of the second and third lines of defence are merged in their organizations. That includes 30 percent who said all three lines of defence are merged (Exhibit 4).

In the latter sort of organization, a single individual not only must attempt to juggle the many duties and activities of two or three separate functions, he or she also must find a way to avoid the inherent conflicts of interest such combined structures present. In actual practice, some executives find it wise to take pains at the beginning of each meeting to declare to other participants which hat they are wearing that day – are they there as the internal auditor or as the vice president of enterprise risk?

Exhibit 4: Organization of Risk Management Functions

In your organization, what is the organization of functions dedicated to the overall risk management framework (internal audit, risk management, internal control)?



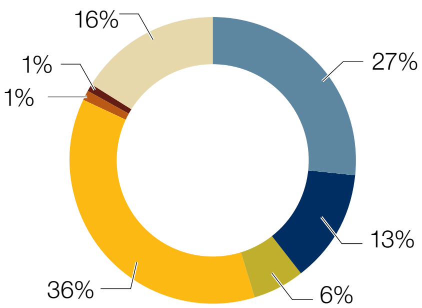
Moreover, it should be noted that financial institutions are required by regulation to maintain separate internal audit, internal control, and risk management functions. It is virtually certain, therefore, that the proportion of the participants who work in combined functions would be even greater were it not for the relatively high number of financial institutions in the survey population.

The reason for companies' tendency to merge these functions is understandable – they need a holistic view of risk: the functions share many of the same issues and employ similar tools, so it is natural to look for opportunities to combine activities and minimize internal bureaucracies. Yet the responses to other questions suggest that in many cases these desired efficiencies are not being achieved, despite the merging of two or all three lines of defence.

For example, when asked if they share common framework elements – such as risk universe, policies, processes, and controls – with other risk management stakeholders, only 36 percent of the survey respondents said that such elements were shared by all three lines of defence (Exhibit 5).

Exhibit 5: Sharing of Common Frameworks

Do you share common frameworks (policy and procedures, process schemes, risk universe, key controls, etc.) with other risk management stakeholders?



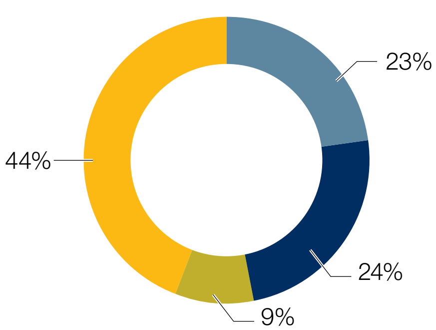
- No, specific to each stakeholder
- Yes, shared between risk management and internal control
- Yes, shared between internal audit and internal control
- Yes, shared between internal audit, risk management, and internal control
- Yes, shared with compliance
- Yes, shared with ethics
- Yes, shared with quality
- Yes, shared with environment, health, and safety
- Other

More than a quarter (27 percent) reported no sharing whatsoever, while 19 percent reported limited sharing of frameworks. Significantly, only 2 percent share common frameworks with related functions such as compliance; ethics; quality; and environment, health, and safety. This speaks to a particular lack of collaboration with the first line of defence – the day-to-day operational management of the organization.

This is reflected in answers to another question, which arguably could be even more significant. When asked who in their organizations actually use the overall risk management framework, nearly half of the respondents (47 percent) said that their operational managers don't use their companies' risk management frameworks (Exhibit 6).

Exhibit 6: Use of Risk Management Framework

Who uses the overall risk management framework within your organization?



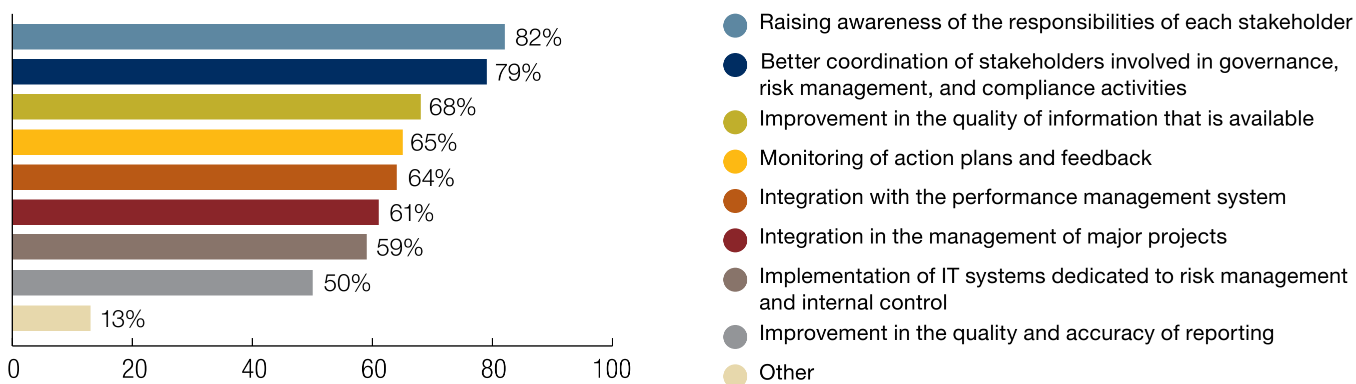
- The various risk management functions
- The risk management functions and general management
- The risk management functions and operational management
- All stakeholders (including operational management)

This is striking when considering that the concepts of enterprise risk management first gained widespread prominence in the 1990s and were further enhanced with the first edition of the COSO Enterprise Risk Management—Integrated Framework. More than 20 years later, just over half (53 percent) of the survey respondents said that their operational management makes use of their risk management framework. This suggests that, in many cases, risk management functions still operate in discrete silos, and risk management is unlikely to be fully embedded in the broader corporate culture. (See the next section of this report.)

The survey participants themselves appeared to recognize the need to maintain clarity and coordination among the three lines of defence. In the section of the survey devoted to risk management practices, the participants were asked the ultimate "bottom line" question: What changes would you like to make to your risk management and internal control organization? The two leading answers were "raising awareness of the responsibilities of each stakeholder" and "better coordination of stakeholders involved in governance, risk management, and compliance activities" (Exhibit 7).

Exhibit 7: Suggested Changes to Risk Management and Internal Control

What change(s) would you like to make to your risk management and internal control organization? (Please select all that apply.)



With so many organizations in which the distinctions among the lines of defence are blurred, maintaining clarity about specific responsibilities is challenging. At the same time, it appears, merging of the three functions has not yet led to achieving better coordination and efficiency. Organizations need to persist with these transformation initiatives. Coordinating the various lines of defence functions to master risk – while maintaining clear lines of accountability for their separate responsibilities – is obviously an ongoing concern and a top priority for the survey participants.

Recommendation: Consider, as a way to achieve transformation, bringing focus to the integration and coordination points that are important to each risk management function and see that each function's needs are addressed when designing commonality and consistency (including enabling governance, risk, and compliance (GRC) systems).

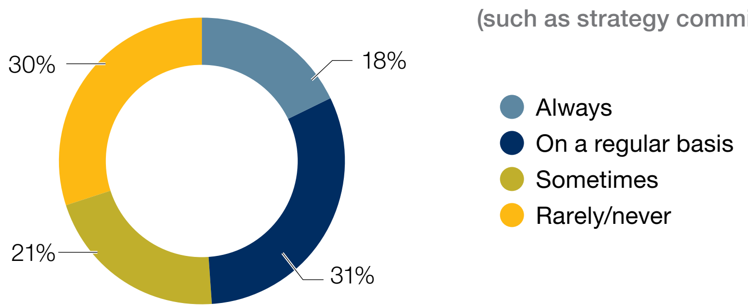
Improvement Opportunity 2: Taking a More Strategic Approach to Risk Management

One of the underlying goals of any risk management framework is to embed an awareness and understanding of risk into the broader corporate culture. This implies the need for risk management concerns to be considered not only in the business-as-usual, day-to-day operations of the organization, but also the need for risk factors to be involved at the strategic level. Logically, it would seem the audit committee would play a leading role in this effort, but the survey results suggest this is not as common as might be expected.

When asked how often risk management functions participate in strategic decision-making bodies, only 18 percent of the respondents said they are always involved. Moreover, nearly a third (30 percent) of the participants said that the risk management functions are rarely or never involved in such decisions (Exhibit 8).

Exhibit 8: Risk Management in Strategic Decision-Making

How often do one or more functions of the risk management framework participate in a strategic decision-making body (such as strategy committee, investment committee)?

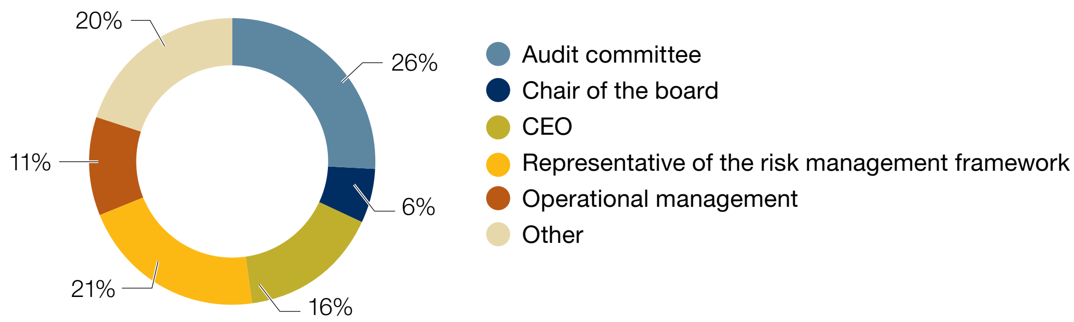


Again, it is likely that the numbers would show an even lower level of involvement were it not for the large number of financial institutions represented in the survey. Because of regulatory requirements, risk management functions are generally well-placed in financial institutions – in fact, banking and related businesses might be able to provide some useful examples for other industries to consider in order to improve risk management's involvement at the strategic level.

Many readers may not find risk management functions' relatively low involvement in strategic issues surprising, given that in many companies risk management does not have a top-level sponsor. When asked to identify the main sponsor of the overall risk management framework in their organizations, less than half of the respondents identified someone at the top executive or board level (audit committee, board chair, or CEO). In many cases, the chief sponsor was someone from within the risk management framework or operational management (Exhibit 9).

Exhibit 9: Main Risk Management Sponsor

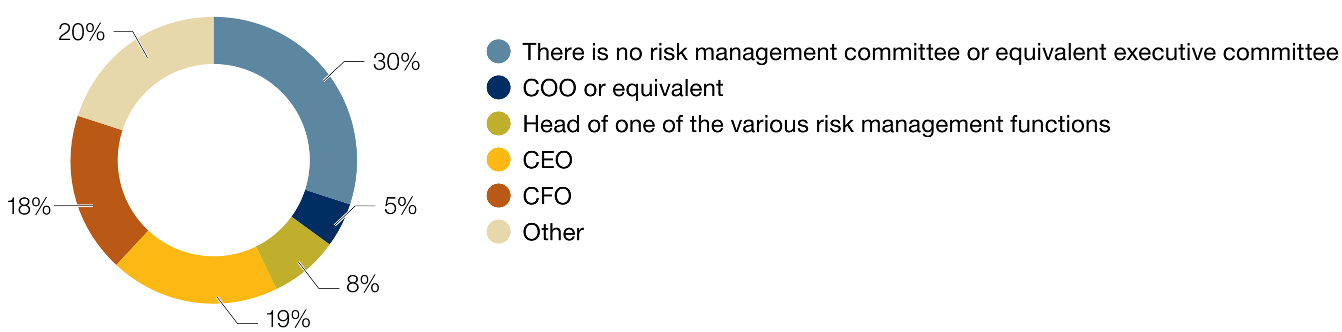
Who is the main sponsor of the overall risk management framework in your organization?



Without a sponsor at the highest levels, the risk management framework may not have the necessary board and executive support to be fully effective in mastering risk. This conclusion is consistent with the findings of another survey question, which suggests that many companies that have chosen to operate with a risk management committee do not enjoy high-level engagement and leadership (Exhibit 10).

Exhibit 10: Risk Management Committee Leadership

Who chairs the risk management committee (or equivalent executive committee)?

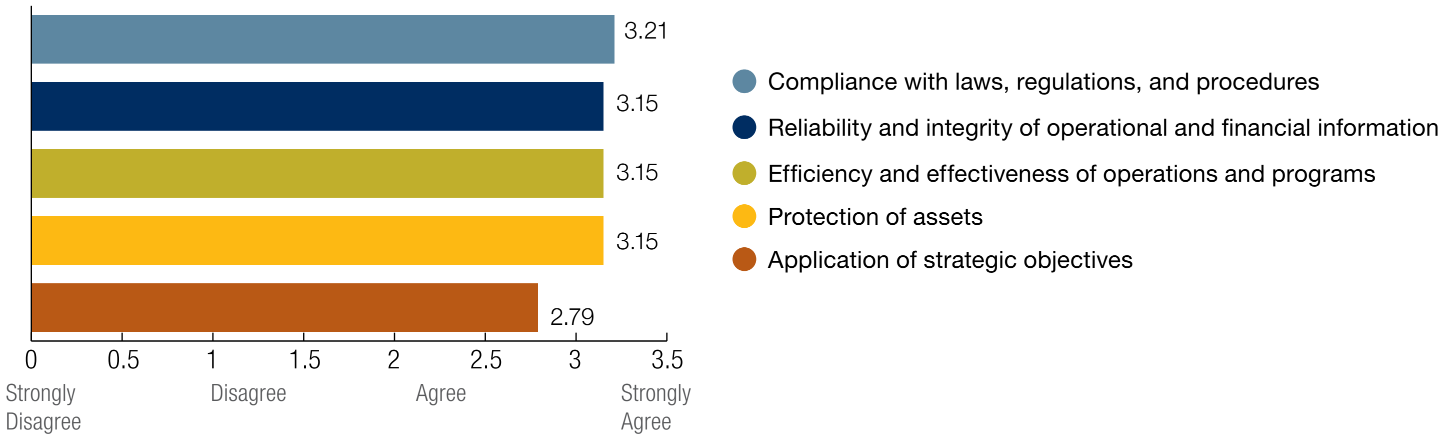


Thirty percent of the respondents said that their organizations do not even have such a committee, and another 20 percent said that the committee is not headed by a C-level executive. Put another way, half of the survey respondents said that their companies do not assign top-level executive resources to heading the risk management committee.

Similar conclusions are suggested by other survey questions, such as those that looked into the role of internal audit specifically. Here again, the responses suggest that this third line of defence often focuses less on issues of strategic impact; instead it concentrates more effort on operational, financial, and compliance-related concerns (Exhibit 11).

Exhibit 11: Internal Audit Focus

Your organization's internal audit work provides an ongoing assessment of: (Please select all that apply.)

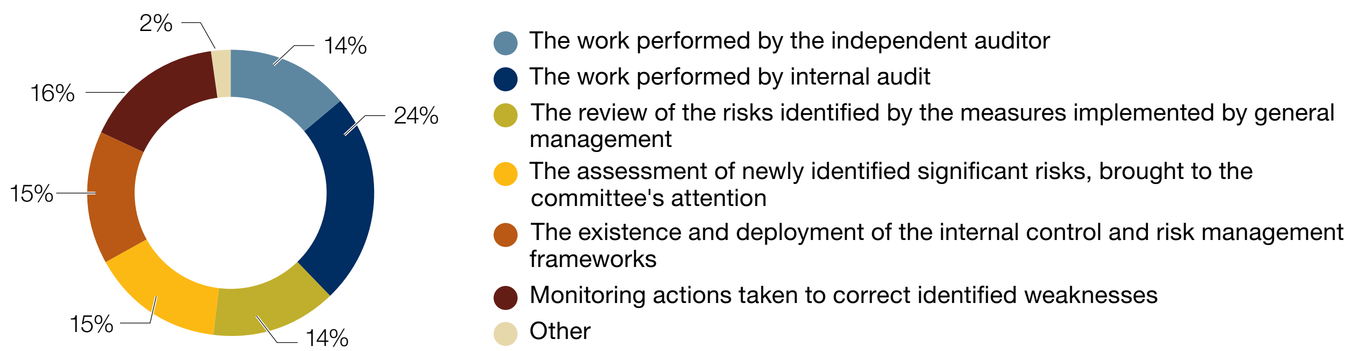


In some ways, the lower level of emphasis on applying strategic objectives is understandable, since compliance, asset protection, and operational and financial issues can be audited much more directly and objectively. But another contributing factor must also be considered: the tone and direction set by the CEO, executive management, and the audit committee itself.

According to the survey participants, their audit committees' focus centered primarily on tactical and operational issues and the direct supervision and monitoring of specific risk-related functions. Topics that could be characterized as more strategic in nature – such as assessing newly identified risks and overseeing the existence and deployment of the internal control and risk management framework – received only about 30 percent of the committee's attention, in the view of the survey participants (Exhibit 12).

Exhibit 12: Audit Committee Focus

In your opinion, the audit committee's effort in terms of overseeing the effectiveness of the internal control and risk management systems is focused on:



These responses are consistent with the opportunity suggested in the previous section of this report – the opportunity to increase risk management effectiveness by clarifying specific responsibilities while at the same time improving coordination among the three major lines of defence functions. Such clarification and coordination could help relieve the audit committee from some of its focus on the day-to-day, business-as-usual functions of the risk management process, enabling the committee to take a more strategic view and devote more attention to emerging issues and the overall enhancement of the enterprisewide risk management effort.

Ultimately, it is the CEO, with direction from the audit committee, and senior management that must take the lead in mastering risk.

Recommendation: Consider positioning the risk management functions to perform the strategic threat analysis as part of the strategic planning (strengths, weaknesses, opportunities, and threats (SWOT) analysis, for example) or stress-testing approaches.

Improvement Opportunity 3: Demonstrating Results and a Positive ROI

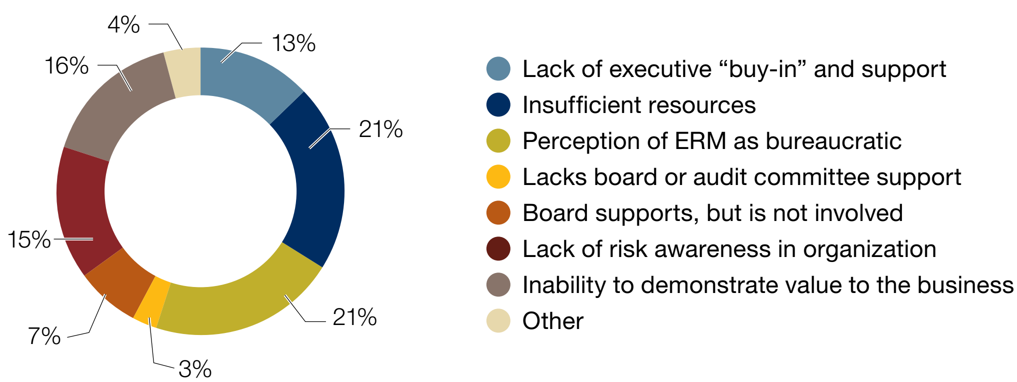
If embedding risk management principles into the culture of the organization is important – and few would argue that it is not – then the obvious question is what is preventing that from happening? Ironically, it could be that one of the impediments to the development of a risk culture is the concept of three lines of defence. The terminology itself is obviously defencive, which can make it seem like a difficult fit in organizations that are more growth-oriented and inherently have a higher risk tolerance.

As a result, the elements of the risk management framework often are regarded as primarily a compliance concern. That, in turn, implies that the investments and resources required to carry them out are regarded as basically just a cost of doing business – a cost that is to be minimized whenever possible. It should come as no surprise, therefore, that internal audit and risk management teams so often feel they are stretched thin and constrained by a lack of resources.

The survey results are consistent with this point of view. When the survey respondents were asked to identify obstacles to implementing the risk management framework, the top two answers were insufficient resources and the perception of enterprise risk management (ERM) as a bureaucratic function (Exhibit 13).

Exhibit 13: Obstacles to Risk Management Implementation

In your opinion, what are the main obstacles to implementing the overall risk management framework?



In fact, virtually all of the obstacles listed in the question are direct consequences of the third-most-cited answer: an inability to demonstrate value to the business. It would seem that overcoming this obstacle would greatly enhance the organization's ability to address the other challenges, such as lack of board support and involvement, lack of executive buy-in, and low risk awareness throughout the organization.

Of course, to some extent the reverse is also true: lack of resources and high-level support can make it more difficult to demonstrate risk management's value to the business. Nevertheless, it seems clear that to gain wider support – and ultimately to be more effectively embedded into the culture of the organization – the centrally coordinated risk management methods must be able to demonstrate they make a positive contribution to the organization's goals and objectives.

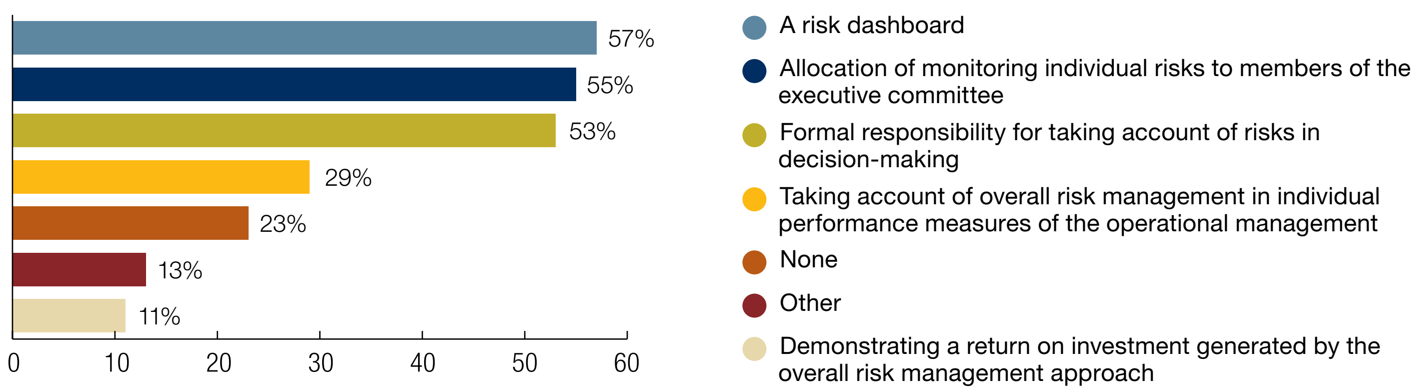
Such positive contributions are not measured exclusively in financial metrics. Contributing to the achievement of strategic goals, or supporting project outcomes, can also be cited as positive contributions – but to be cited they must first be monitored and measured.

This can be challenging, of course. For example, how can risk managers quantify the losses that were prevented by making sure the organization was not the victim of a cybersecurity incident? Researching and tracking the losses incurred by comparable organizations with similar risks is one way to begin quantifying risk management's contribution. Reducing global insurance premiums by demonstrating good risk management to your broker, is another.

The difficulty of the task is reflected in the fact that very few of the survey respondents expressed belief that they are achieving it. When asked which differentiating factors they have implemented to support more effective risk management activities, only a handful of the respondents cited efforts to demonstrate a positive ROI (Exhibit 14).

Exhibit 14: Differentiating Factors

Which differentiating factors have you implemented in order to ensure effective operations of risk management activities? (Please select all that apply.)



Developing risk dashboards, assigning formal responsibility and accountability for risk, and incorporating risk into management performance measures and other existing business processes, such as budgeting and capital expenditures management, are comparatively easier techniques to implement, and thus are more widely used for improving the effectiveness of risk management functions.

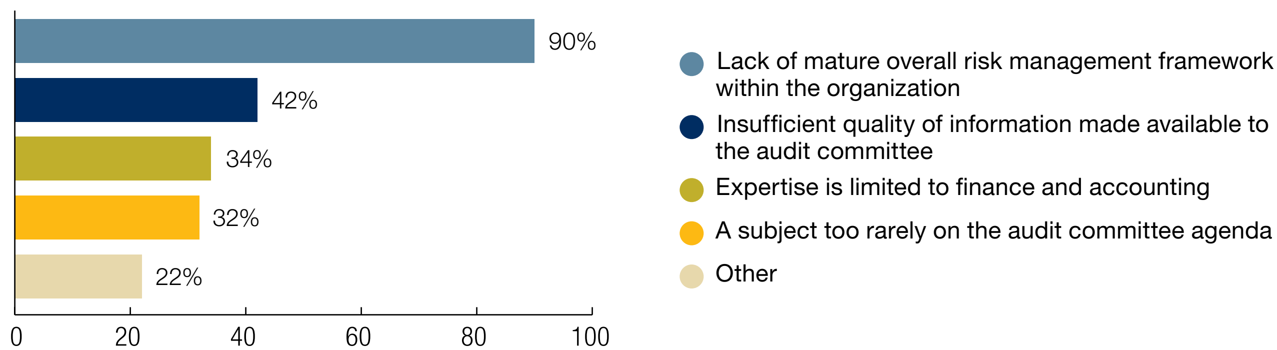
Improvement Opportunity 4: The Board and Senior Management as Risk Culture Champions

Of the various survey questions explored in this report, one of the most revealing is the listing of perceived obstacles to implementing the overall risk management framework (Exhibit 13). The question is particularly helpful if the obstacles listed are regarded not just as impediments but also as areas where improvement can be made. In other words, improved executive buy-in and support can help overcome the lack of resources, just as the ability to demonstrate value can help overcome negative perceptions of the ERM process.

A similar constructive approach can be applied to a related survey question that focused particularly on the role of the audit committee. Respondents were asked to identify the main obstacles that prevent more effective audit committee oversight of the internal control and risk management frameworks. In other words, what factors work to inhibit its oversight of the three lines of defence (Exhibit 15)?

Exhibit 15: Audit Committee Obstacles

In your opinion, what are the main obstacles to oversight of the internal control and risk management frameworks by the audit committee? (Please select all that apply.)

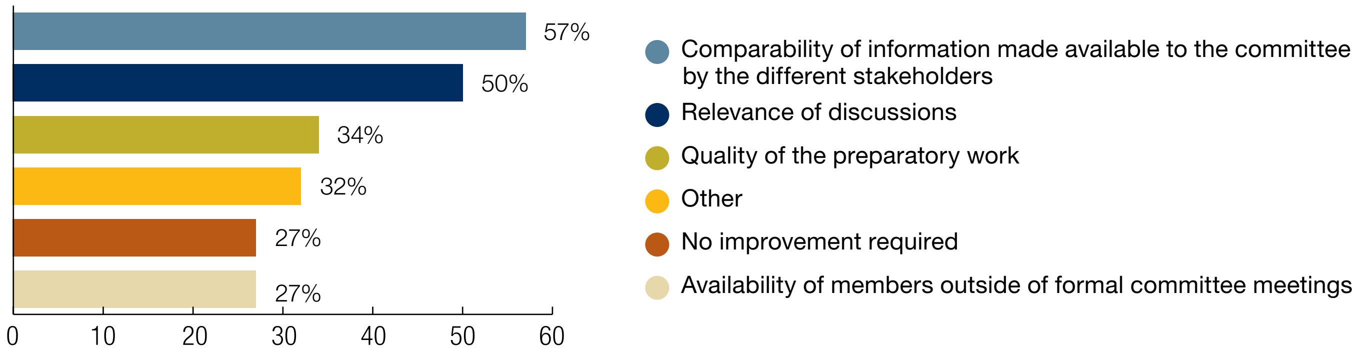


By far the most cited obstacle was the lack of a mature overall risk management framework. As in the earlier question, the solutions to this obstacle could actually be found in some of the other responses. That is, the maturity of the risk management framework can be greatly enhanced by improving the quality of information provided to the audit committee, broadening the committee's expertise beyond the finance and accounting disciplines, and directly addressing such subjects on the audit committee agenda.

In addition, the participants were asked directly to identify ways audit committees could be more effective. Bear in mind that none of the survey respondents were audit committee members; rather, the survey population consisted primarily of individuals who report to and work with their audit committees. Their responses indicate their perceptions of their interactions with the committee and suggest several important opportunities for improvement (Exhibit 16).

Exhibit 16: Audit Committee Improvements

In your opinion, what are the necessary improvements to the oversight of the internal control and risk management systems by the audit committee? (Please select all that apply.)



The method recommended most often for improving audit committee oversight is to enhance the comparability of information from various stakeholders. This is consistent with the earlier observation about the need for better coordination among the three lines of defence, which are the primary stakeholders involved here.

The next-highest response suggests a perception that committee members are not as focused as they could be, particularly in terms of asking questions that are relevant to the risks being discussed and their relative importance to the organization's overall risk exposure.

Recommendation: Consider undertaking and presenting the results of culture surveys to the board or audit committee, or put risk tolerance and appetite on the agenda. Alternatively, have the board be responsible for risk oversight, with delegation, when appropriate, of certain specific risks to board subcommittees (perhaps the health, safety and environment subcommittee or the human resources risks subcommittee).

Conclusion: Responsibilities and Tools for Establishing a Mastering Risk Culture

It should be noted that the issues indicated by the survey respondents are comparable to those cited by participants in other similar surveys in recent years. When survey participants are asked about current and upcoming risk initiatives in their organizations, improving the risk culture and the formal incorporation of risk into strategic planning issues are commonly listed as high priorities.

Organizations can get on the right track by continuing to focus on the four broad areas of opportunity identified in this report by:

1. Clarifying and coordinating roles and responsibilities in the three lines of defence model
2. Elevating the role of risk to a more strategic level
3. Developing ways to demonstrate risk management's positive contribution to organizational goals
4. Working with the board or audit/risk committee(s) and senior management to improve the risk culture

In this way, internal auditors and other risk professionals can improve the effectiveness of their risk organizations and enhance the perceptions of their profession as a whole.

Although it's not easy to do, tremendous value can be unlocked if management can truly master risks rather than try to manage them when they arise. We recommend that companies tackle these themes in the interest of sustaining their risk management approach and their enterprise.

About IIA Canada

http://www.iiacanada.ca

The Institute of Internal Auditors Canada (IIA Canada) serves the needs of more than 7,600 members in Canada. With its headquarters in Ottawa, IIA Canada works in partnership with its 12 chapters across the nation, providing training, publications, and services for its members, and advocating for the profession to key government and regulatory bodies and related organizations. IIA Canada is affiliated with the global Institute of Internal Auditors, which serves 180,000 members in 190 countries.

Crowe Horwath Global Risk Consulting

Crowe Horwath Global Risk Consulting, a member of Crowe Horwath International, a top 10 global accounting and consulting network, is a leading risk consulting provider with member firms in more than 120 countries around the world. Our experienced professionals have deep subject-matter expertise in risk management, internal audit, fraud and ethics, security and privacy, and regulatory compliance to keep you advised of emerging trends, industry benchmarks, and best practices. For more information, visit www.crowehorwath.net/risk.

Contact Information

Jim Barbour is managing director, Canada, at Crowe Horwath Global Risk Consulting. He can be reached at +1 416 963 7118 or jim.barbour@crowehorwath.com.

Jonathan Burnett is CEO of Crowe Horwath Global Risk Consulting. He can be reached at +33 1 53 53 03 92 or jonathan.burnett@crowehorwath.com.

Sheila Smigarowski is past chairman of IIA Canada and an internal audit and risk management executive. She can be reached at +1 780 868 6292 or ssmigarowski@telus.net.

Mike Varney is a partner and Americas regional lead with Crowe Horwath Global Risk Consulting. He can be reached at +1 216 623 7553 or mike.varney@crowehorwath.com.

[1] "The Three Lines of Defense in Effective Risk Management and Control," IIA Position Paper, January 2013, https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

[2] See Douglas J. Anderson and Gina Eubanks, "Leveraging COSO Across the Three Lines of Defense," joint publication of IIA and COSO, July 2015, http://www.coso.org/documents/COSO-2015-3LOD-PDF.pdf