Who Owns Risk?

A Look at Internal Audit's Changing Role

RISK

Core Report

Paul J. Sobel
CIA, QIAL, CRMA

The IIA Research Foundation

CBOK
The Global Internal Audit Common Body of Knowledge

About CBOK

SURVEY FACTS

Respondents	14,518*
Countries	166
Languages	23

EMPLOYEE LEVELS

Chief audit executive (CAE)	26%
Director	13%
Manager	17%
Staff	44%

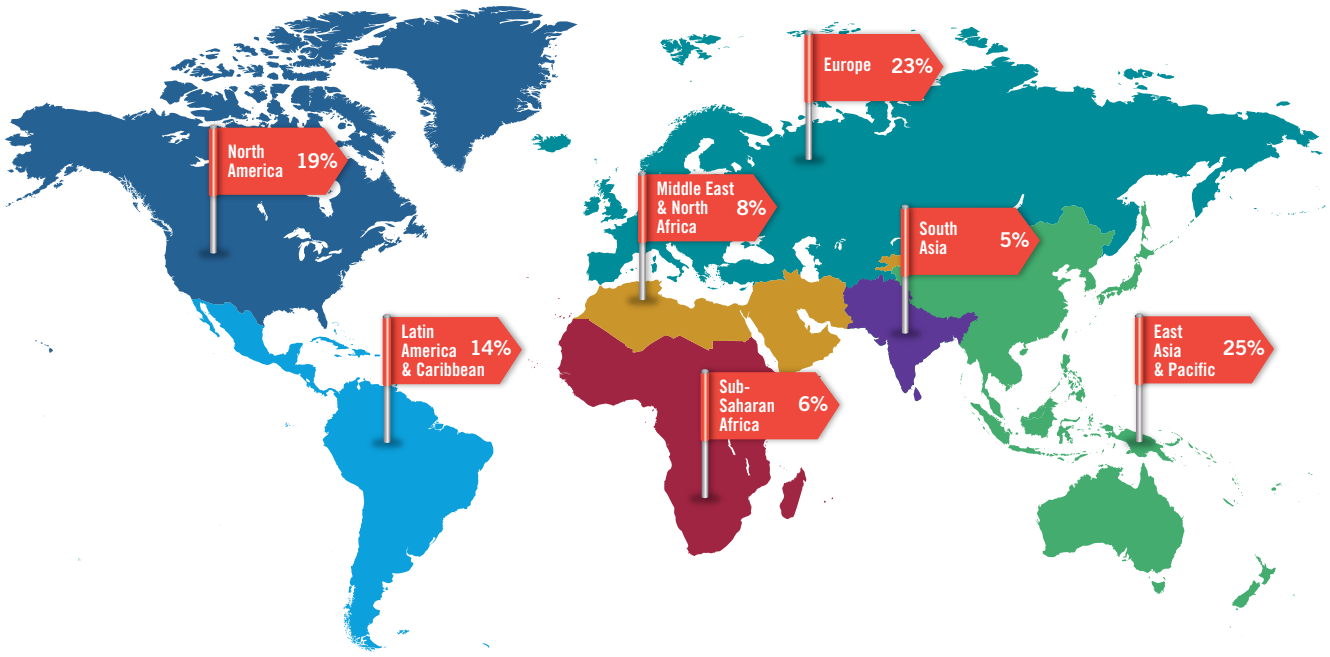
*Response rates vary per question.

The Global Internal Audit Common Body of Knowledge (CBOK) is the world's largest ongoing study of the internal audit profession, including studies of internal audit practitioners and their stakeholders. One of the key components of CBOK 2015 is the global practitioner survey, which provides a comprehensive look at the activities and characteristics of internal auditors worldwide. This project builds on two previous global surveys of internal audit practitioners conducted by The IIA Research Foundation in 2006 (9,366 responses) and 2010 (13,582 responses).

Reports will be released on a monthly basis through July 2016 and can be downloaded free of charge thanks to the generous contributions and support from individuals, professional organizations, IIA chapters, and IIA institutes. More than 25 reports are planned in three formats: 1) core reports, which discuss broad topics, 2) closer looks, which dive deeper into key issues, and 3) fast facts, which focus on a specific region or idea. These reports will explore different aspects of eight knowledge tracks, including technology, risk, talent, and others.

Visit the CBOK Resource Exchange at www.theiia.org/goto/CBOK to download the latest reports as they become available.

CBOK 2015 Practitioner Survey: Participation from Global Regions



Note: Global regions are based on World Bank categories. For Europe, fewer than 1% of respondents were from Central Asia. Survey responses were collected from February 2, 2015, to April 1, 2015. The online survey link was distributed via institute email lists, IIA websites, newsletters, and social media. Partially completed surveys were included in analysis as long as the demographic questions were fully completed. In CBOK 2015 reports, specific questions are referenced as Q1, Q2, and so on. A complete list of survey questions can be downloaded from the CBOK Resource Exchange.

CBOK Knowledge Tracks

Future

Global Perspective

Governance

Management

Risk

Standards & Certifications

Talent

Technology

Contents

Executive Summary

Who really owns risk? The literal answer is "not internal audit." However, there is no question that internal audit has helped organizations better understand and manage risk in the past and will undoubtedly play a valuable role in the future.

This report not only provides insights into the status of risk management and the role of internal audit around the world, but it also lays out 13 key actions that can help chief audit executives (CAEs) and internal auditors ensure that their internal audit function is properly positioned to address risk challenges in an ever-changing world.

Using survey findings from this report, you will be able to compare your risk-related practices to others around the world and in different industries. You will gain new insights about:

- Your organization's risk practices
- Your interaction with enterprise risk management (ERM)
- Your level of responsibility for risk assessment in your organization
- Your level of risk maturity
- Your risk assessment proficiency

This report was written by Paul Sobel, the 2013–2014 chairman of the Board of Directors of The IIA and well-known author and speaker on risk and internal audit topics. Current information about risk practices was obtained from the CBOK 2015 Global Internal Audit Practitioner Survey, the largest ongoing survey of internal auditors in the world. These findings were supplemented with interviews of global internal audit and risk leaders to obtain regional context.

Introduction

MISSION OF INTERNAL AUDIT

"To enhance and protect organizational value by providing stakeholders with risk-based, objective and reliable assurance, advice, and insight."

—From the revised IPPF, The Institute of Internal Auditors, July 2015

The recently updated International Professional Practices Framework (IPPF) includes a new mission for internal auditing: "To enhance and protect organizational value by providing stakeholders with risk-based, objective and reliable assurance, advice, and insight." To fulfill that mission, internal audit functions across the globe must focus on risk as the foundation for what should be audited, how it should be audited, and what should be reported.

The CBOK 2015 Global Internal Audit Practitioner Survey provides data and insight that will help internal auditors understand the global practices around risk. After first understanding the extent to which formal risk management is in place (chapter 1), this report looks at internal audit's positioning within risk management (chapter 2). The Three Lines of Defense Model helps to understand this positioning because it distinguishes between management's responsibilities for managing risk (first line of defense), other functions' role in supporting and overseeing risk management (second line), and internal audit's role of providing objective assurance (third line).*

Chapter 3 looks at internal audit's risk management responsibilities, with particular focus on its assurance responsibilities. Finally, chapter 4 covers a variety of topics relating to internal audit's use of risk, including attributes of risk assessment, which helps shape the internal audit plan, other resources for the audit plan, and risk management competency levels of internal auditors.

It is clear that advancements have been made in risk management, and internal audit's role continues to evolve. However, there are many opportunities for CAEs and other internal auditors to ensure their internal audit functions can effectively address risk challenges in an ever-changing world. The key actions identified throughout this report should help address these opportunities.

---

* For additional information, refer to The IIA's Position Paper, The Three Lines of Defense in Effective Risk Management and Control, January 2013, and "Leveraging COSO Across the Three Lines of Defense," produced in partnership by The IIA and COSO, January 2015.

1 Trends in Risk Management

Risk management continues to grow and evolve around the world. The global financial crisis that began in 2008 demonstrated the value and importance of good risk management practices. Since then, regulations have been promulgated that require risk management, or components of it, and much has been written about ways to manage risk in a rapidly changing, global economy.

Formal Risk Management Processes

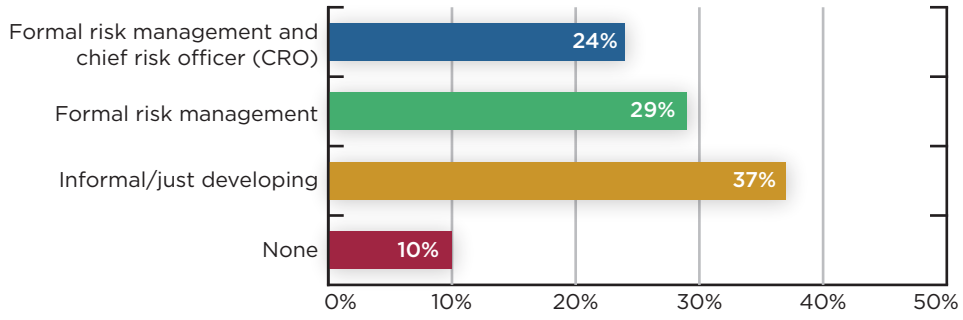
The 2015 CBOK survey results show that more than half the CAEs from around the world believe that formal risk management processes and procedures are in place in their organizations (see **exhibit 1**). As shown in this chart, more than half (53%) indicate that "formal risk management processes and procedures are in place" (29%) or "the organization has a formal enterprise risk management process with a chief risk officer or equivalent" (24%). While a slight majority believe their organizations have formal risk management processes, one has to wonder whether there has been continuing risk management growth over time.

Trends Over Time

While there are few surveys that ask the same questions about risk over time, some resources can offer glimpses into the growth of risk management:

- The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) 2010 *Report on ERM* identified that only a little more than a quarter of the 460 respondents considered their risk management program to be a "systematic, robust, and repeatable process

Exhibit 1 Risk Management Practices



Note: Q58: What is your organization's level of development for its risk management processes? CAEs only. *n* = 2,709.

> *"The Basel regulations and Solvency II Directive have been important drivers in the development of independent risk management and compliance functions for banks and insurance companies in Europe."*
>
> —Charlotta Löfstrand-Hjelm, Chief Internal Auditor, Länsförsakringar (LFAB), Stockholm, Sweden

with regular reporting of aggregate top risk exposures to the board." This study was almost entirely North American-based and included 20% from the financial services sector.

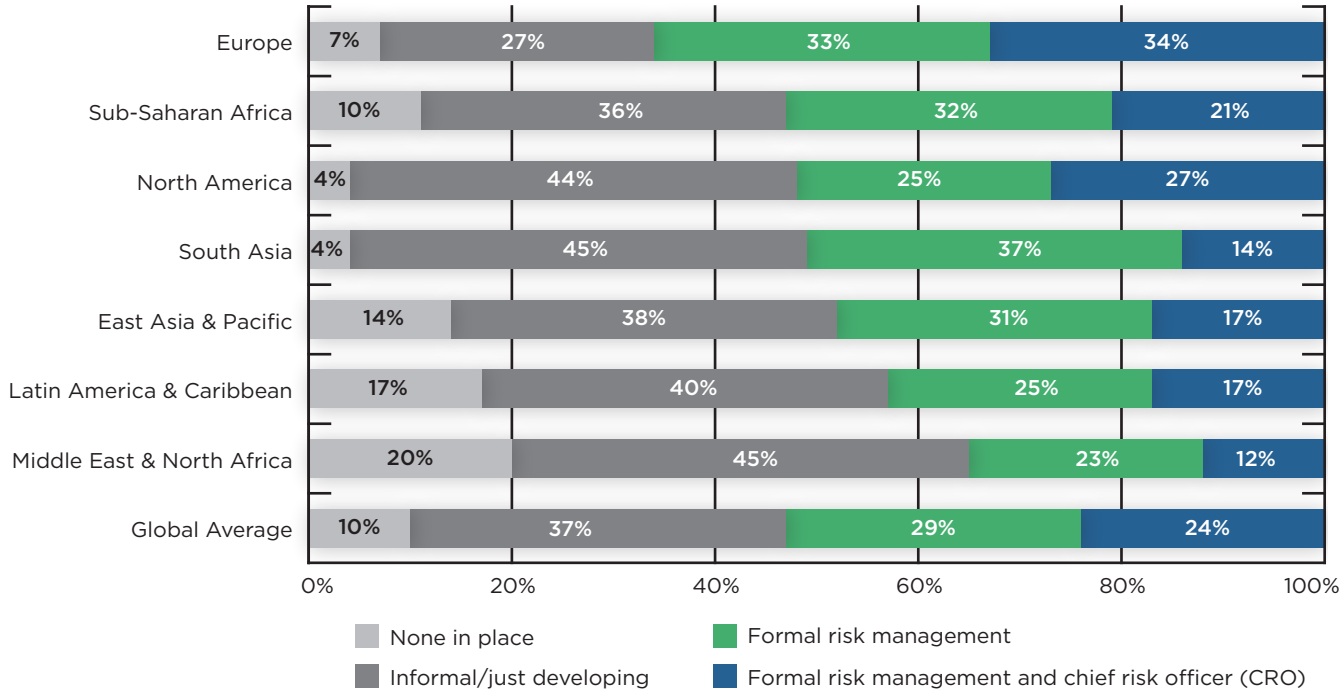
- In 2011, the Risk Management Society (RIMS) published results from its *2011 Risk Benchmark Survey*™ that included responses from 1,431 risk managers, 94% of whom were from North America and 15% from the financial services sector. The survey results showed that more than half (54%) had either a fully or partially integrated risk management program, compared to just over a third in their 2009 survey.
- The International Federation of Accountants (IFAC) issued an information paper in 2011 titled *Global Survey on Risk Management and Internal Control*, in which they reported that two-thirds of the 586 respondents indicated they had a formal risk management system (more than three-quarters were from outside North America and a quarter were from the financial services sector).

A comparison of these studies cannot be considered definitive research into the growth of risk management; however, based on their timing and findings, it appears there was notable growth in formal risk management coming out of the global financial crisis, which is somewhat intuitive. However, that rate of growth may have slowed in recent years. It is also notable that the IFAC paper, which included a much higher proportion of respondents from outside North America, showed a higher rate of formal risk management than did the other two studies.

Region View

The 2015 CBOK survey also shows differences in risk management practices by region (see **exhibit 2**). In particular, a notably higher percentage of CAEs from Europe indicate a formal risk management process is in place (67%), which mirrors the IFAC results from 2011. Conversely, only 35% of Middle East & North Africa respondents and 42% of Latin America & Caribbean respondents indicate a formal risk management process is in place. A response to the findings from Europe was obtained from Charlotta Löfstrand-Hjelm, chief internal auditor, Länsförsakringar (LFAB), Stockholm, Sweden, who has experience in the insurance industry. She observed that regulations in the financial services sector have accelerated the development of independent risk management functions in Europe. However, such regulations are less prevalent in the Middle East & North Africa and the Latin America & Caribbean regions; hence, the lower results from those regions. Interviewees from those regions emphasized that formal risk management tends to reside only in very large companies, the financial services sector, and subsidiaries of foreign companies.

Exhibit 2 **Risk Management Practices (Region View)**



Note: Q58: What is your organization's level of development for its risk management processes? CAEs only. *n* = 2,675. Due to rounding, some region totals may not equal 100%.

KEY ACTION 1

Be advocates for the advancement of formal risk management processes, regardless of industry.

Industry View

Variations among industries likely are also related to the level of regulation. Because of the regulations promulgated after the global financial crisis, one might hypothesize that a greater percentage of finance and insurance companies would have implemented risk management. The data proves that to be true, as almost three-quarters of finance and insurance companies have formal risk management processes in place (see **exhibit 3**). It is not surprising that an industry that is heavily regulated would have a higher percentage of formal risk management processes in place, particularly since, in many countries, finance and insurance companies are required to have a certain level of risk management. It is interesting to note that if responses for all nonfinancial industries are combined, an average of only 45% have formal risk processes, indicating that in the absence of regulation, a majority of organizations have not yet moved to a formal risk management state (see **exhibit 4**).

Size View

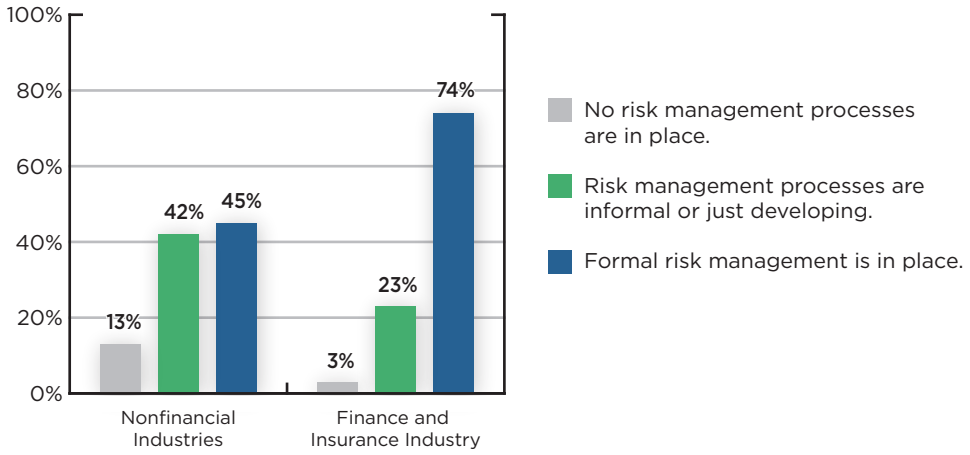
Finally, one might expect larger companies to have more formal risk management processes than smaller companies. This expectation arises for two reasons: 1) larger companies have more resources to devote to risk management, and 2) most financial institutions are larger. The data proves this out, with

Exhibit 3 Formal Risk Management Practices (Industry View)

Finance and insurance	74%
Mining, quarrying, and oil and gas extraction	56%
Utilities	56%
Professional, scientific, and technical services	55%
Real estate and rental and leasing	50%
Construction	49%
Wholesale trade	47%
Public administration	46%
Health care and social assistance	45%
Manufacturing	44%
Other services (except public administration)	43%
Transportation and warehousing	42%
Information	42%
Retail trade	42%
Other	37%
Educational services	31%
Average	53%

Note: Q58: What is your organization's level of development for its risk management processes? Exhibit shows respondents who chose the option "Formal risk management processes and procedures are in place" or "The organization has a formal enterprise risk management (ERM) process with a chief risk officer or equivalent." CAEs only. *n* = 2,709.

Exhibit 4 Risk Management Practices (View by Financial vs. Nonfinancial Industries)



Note: Q58: What is your organization's level of development for its risk management processes? CAEs only. *n* = 2,709.

KEY ACTION 2

Seek opportunities to help expedite the implementation of formal risk management, and sustain it when it is already in place.

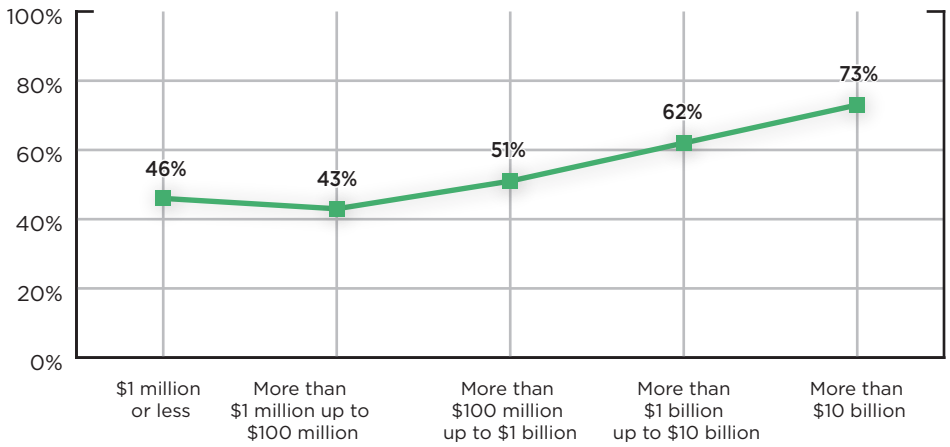
formal risk management processes in place in about 7 out of 10 of the largest companies, compared to about 4 out of 10 of the smallest companies (see **exhibit 5**).

Summary

To summarize, financial institutions and larger companies, many of which are probably the same, show more progress in establishing formal risk management processes. Additionally, companies in Europe have a higher percentage of formal risk management processes, probably reflecting more advanced governance regulations than in other parts of the world. It is important to note that regulations may exist in other parts of the world, such as the U.S. Sarbanes-Oxley Act of 2002. However, these regulations do not require advancement of risk management as a whole; instead, the focus is on risks related to certain areas, such as internal controls over financial reporting. That may explain why the regulations in Europe and certain other parts of the world tend to drive more formal risk management.

It is also important to recognize that formal risk management is not yet present in a global average of 47% of organizations. Based on a variety of survey findings regarding risk, this may reflect a slowdown in the proliferation of risk management implementation subsequent to the period immediately following the global recession, which is somewhat disconcerting. However, CAEs can certainly impact the progress and sustainability of risk management in their organizations.

Exhibit 5 Formal Risk Management Practices (Revenue View)



Note: Q58: What is your organization's level of development for its risk management processes? CAEs only. *n* = 1,996.

2 Internal Audit's Positioning in Risk Management

The Three Lines of Defense Model positions risk management in the second line and internal audit in the third. How closely are internal audit functions around the world aligned with that model?

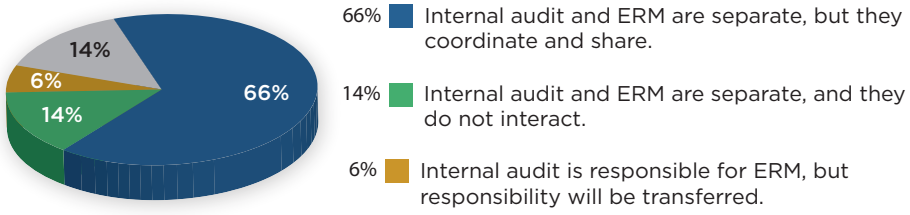
Relationship to ERM

Among all global respondents, 66% indicate that internal audit and ERM are separate functions that coordinate and share knowledge at their organizations (see **exhibit 6**). Another 14% indicate that internal audit and ERM are separate functions and they do not interact. This means that 80% of respondents say their internal audit functions are separate from risk management, which is an encouraging trend because it is an indicator of delineation between the second and third lines of defense. On the other hand, one-fifth of the respondents indicated internal audit is responsible for ERM, and more than two-thirds of those respondents have no plans to transfer it; thus, there is still work to be done to separate these key roles.

Three Lines of Defense

However, for the 66% who coordinate and share information, there may be a caution that such coordination could create some blurring between the second and third lines of defense. Some survey respondents recognize this situation in their organizations. Among survey respondents who use the Three Lines of Defense Model, 13% say the distinction between the second and third lines is not clear (Q63, *n* = 11,255). For more in-depth analysis of survey responses about the Three Lines of Defense Model, please see the CBOK report titled *Combined Assurance: One Language, One Voice, One View*.

Exhibit 6 Relationship Between Internal Audit and Enterprise Risk Management (ERM)



Note: Q59: What is the relationship between internal audit and enterprise risk management (ERM) at your organization? *n* = 9,437.

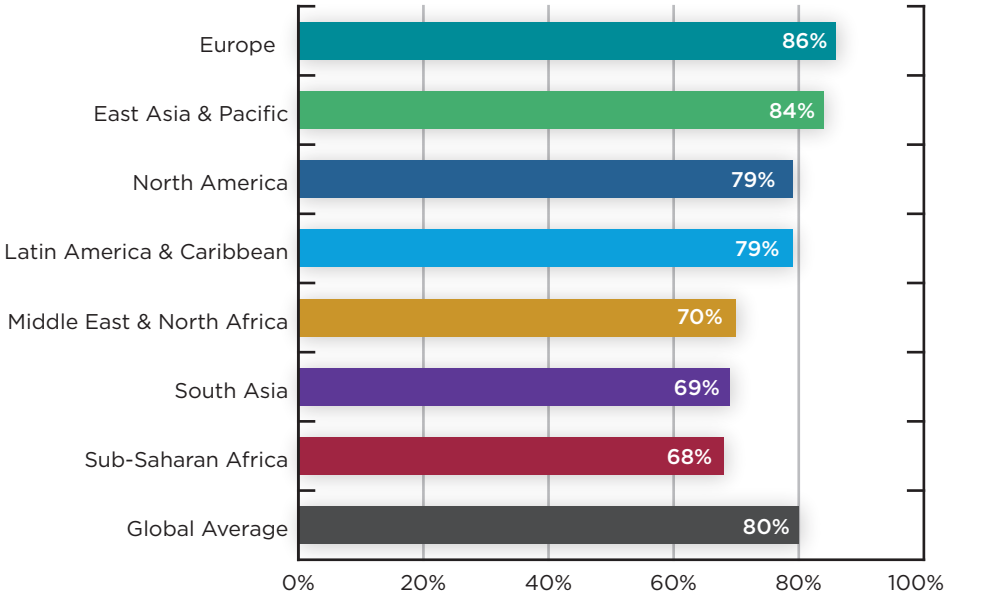
Region View

The separation between internal audit and ERM varies between global regions in some unexpected ways. Europe has the highest percentage of organizations separating internal audit and ERM (86%), which is consistent with the higher level of formal risk management in that region (as discussed in chapter 1). However, the second highest percentage was in East Asia & Pacific (84%) (see **exhibit 7**), but this region was actually below the global average for formal risk management in their organizations. Naohiro Mouri, executive corporate officer/chief internal auditor, AIG Japan Holdings, Tokyo, Japan, speculates that, while formal risk management may not be as prevalent throughout all parts of East Asia & Pacific, there is strong emphasis throughout the region on compliance with The IIA's *International Standards for the Professional Practice of Internal Auditing* (*Standards)* and other guidance, which may drive the higher percentage of separation between internal audit and risk management.

Industry View

Looking at this question from the industry point of view, we find that 93% of finance and insurance respondents say their organizations have separation between internal audit and ERM (see **exhibit 8**). Because finance and insurance companies made up 33% of the total respondents, that industry sector clearly weighted the results toward the

Exhibit 7 Organizations with Internal Audit and ERM Separate (Region View)



Note: Q59: What is the relationship between internal audit and enterprise risk management (ERM) at your organization? Exhibit shows respondents who chose the option "Internal audit and ERM are separate functions and they do not interact" or "Internal audit and ERM are separate functions, but they coordinate and share knowledge." *n* = 9,314.

> *Typically, regulators in the East Asia & Pacific region follow or refer to The IIA's* Standards *and guidance for corporate governance structures; thus, it is prevalent for internal audit to be separate from risk management.*
>
> —Naohiro Mouri, Executive Corporate Officer/Chief Internal Auditor, AIG Japan Holdings, Tokyo, Japan

Exhibit 8 Organizations with Internal Audit and ERM Separate (Industry View)

Finance and insurance	93%
Mining, quarrying, and oil and gas extraction	80%
Public administration	78%
Utilities	78%
Other services (except public administration)	75%
Transportation and warehousing	75%
Information	75%
Professional, scientific, and technical services	74%
Construction	72%
Wholesale trade	70%
Real estate and rental and leasing	69%
Health care and social assistance	68%
Manufacturing	68%
Educational services	67%
Retail trade	64%
Other	63%
Average	80%

Note: Q59: What is the relationship between internal audit and enterprise risk management (ERM) at your organization? *n* = 9,437.

KEY ACTION 3

Work with management and other internal assurance providers to ensure clarity of roles within the three lines of defense.

80% global average. In fact, no other industry sector was even above 80%. This indicates that, in other industries, the distinction between second and third lines of defense may not be as clear.

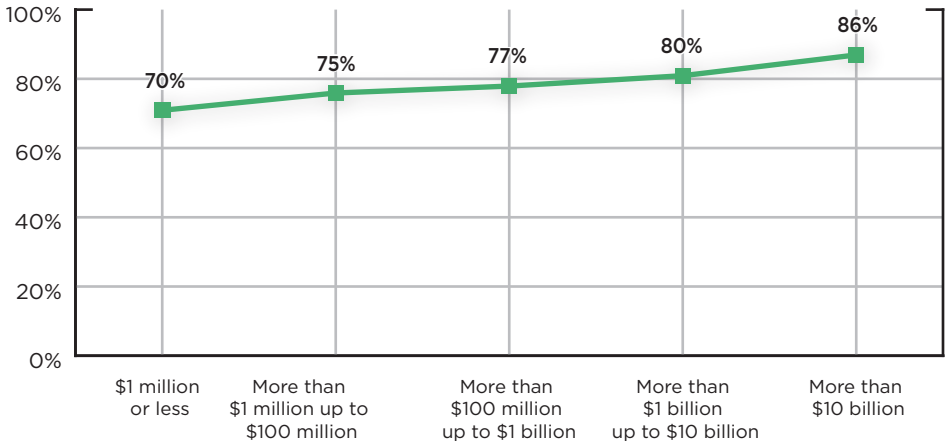
Size View

Larger companies showed higher percentages of separation between the internal audit and risk management functions than did smaller ones (see **exhibit 9**).

Summary

Overall, it appears that there is separation between internal auditing and risk management, particularly in regions where there is more regulation, and most notably among companies in the financial services sector. Also, larger companies tend to have greater separation between the two, which is probably correlated. However, there are some indications that there may be some blurring between the second and third lines of defense, which was also noted in the 2014 Pulse of the Profession survey. This bears watching in the coming years to ensure the valuable roles in those two lines of defense do not become so blurry that the quality and reliability of assurance diminishes.

Exhibit 9 **Organizations with Internal Audit and ERM Separate (Revenue View)**



Note: Q59: What is the relationship between internal audit and enterprise risk management (ERM) at your organization? *n* = 5,008.

3 Internal Audit's Risk Management Responsibilities

Having good separation between internal auditing and risk management sounds like an encouraging and important practice. However, to put the topic from chapter 2 into context, it is important to understand how internal audit's risk responsibilities differ from those of an ERM function. Thus, this chapter provides insights on how internal audit provides assurance and advice related to risk. Internal audit may have various responsibilities for risk (see **exhibit 10**; note that respondents could choose multiple answers to this survey question).

Overall Assurance on Risk Management

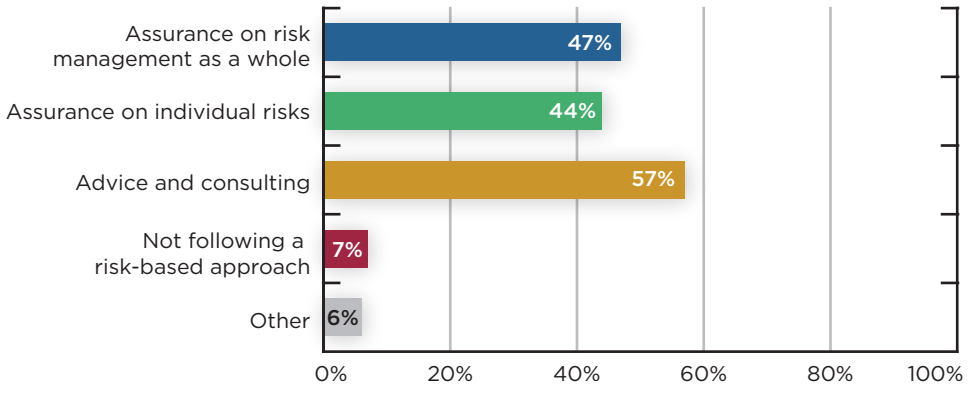
First, it is important to note that 47% of respondents indicate that they provide assurance on risk management as a whole. On one hand, this seems rather high considering the limited guidance available on how to provide such assurance. On the other hand, the results may be low when compared to the 2010 CBOK survey responses. While the questions were not phrased exactly alike, 57% of respondents in 2010 indicated their audit activity conducted audits of ERM processes, and 20% indicated they expected such audits to increase in the next five years (i.e., by 2015).* Even though the question was asked in different ways, the fact that the percentage for risk management assurance was lower in

* *Characteristics of an Internal Audit Activity* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2010), 23–24.

KEY ACTION 4

Strive to provide assurance on risk management as a whole, not just on individual risks.

Exhibit 10 Internal Audit's Risk Management Responsibilities



Note: Q60: What areas of responsibility does internal audit have related to risk at your organization? (Choose all that apply.) *n* = 11,935.

2015 than in 2010 suggests that internal auditors did not increase their risk management assurance in the last five years.

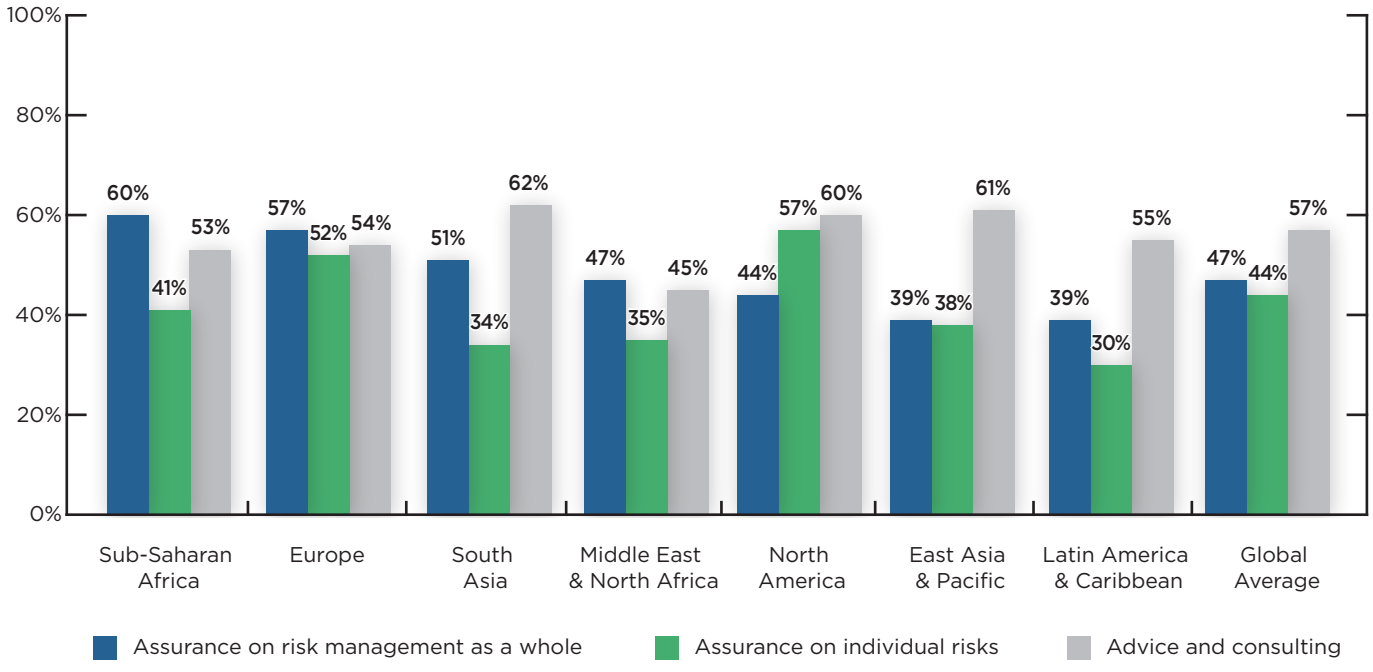
Region View

Looking at the results by region (see **exhibit 11**), 60% of respondents in Sub-Saharan Africa indicate they provide assurance on risk management as a whole, the highest percentage of any region in the world. That is likely due to the strong governance requirements in South Africa, which make assurance on risk management more critical (about 40% of the region's respondents were from South Africa). Europe had the next highest percentage (57%), likely due to the level of regulation and governance focus in that region. Conversely, only 39% of respondents from East Asia & Pacific and Latin America & Caribbean and 44% from North America indicated they provide assurance on risk management as a whole, so such assurance is not yet prevalent in many parts of the world.

Size View

The responses for different size companies are similar to the other survey questions; that is, the larger companies report higher percentages of respondents indicating they provide assurance on risk management as a whole. However, none of these demographic groups was greater than two-thirds, so even very large companies could increase their focus on risk management assurance.

Exhibit 11 **Internal Audit's Risk Management Responsibilities (Region View)**



Note: Q60: What areas of responsibility does internal audit have related to risk at your organization? (Choose all that apply.) *n* = 11,779.

KEY ACTION 5

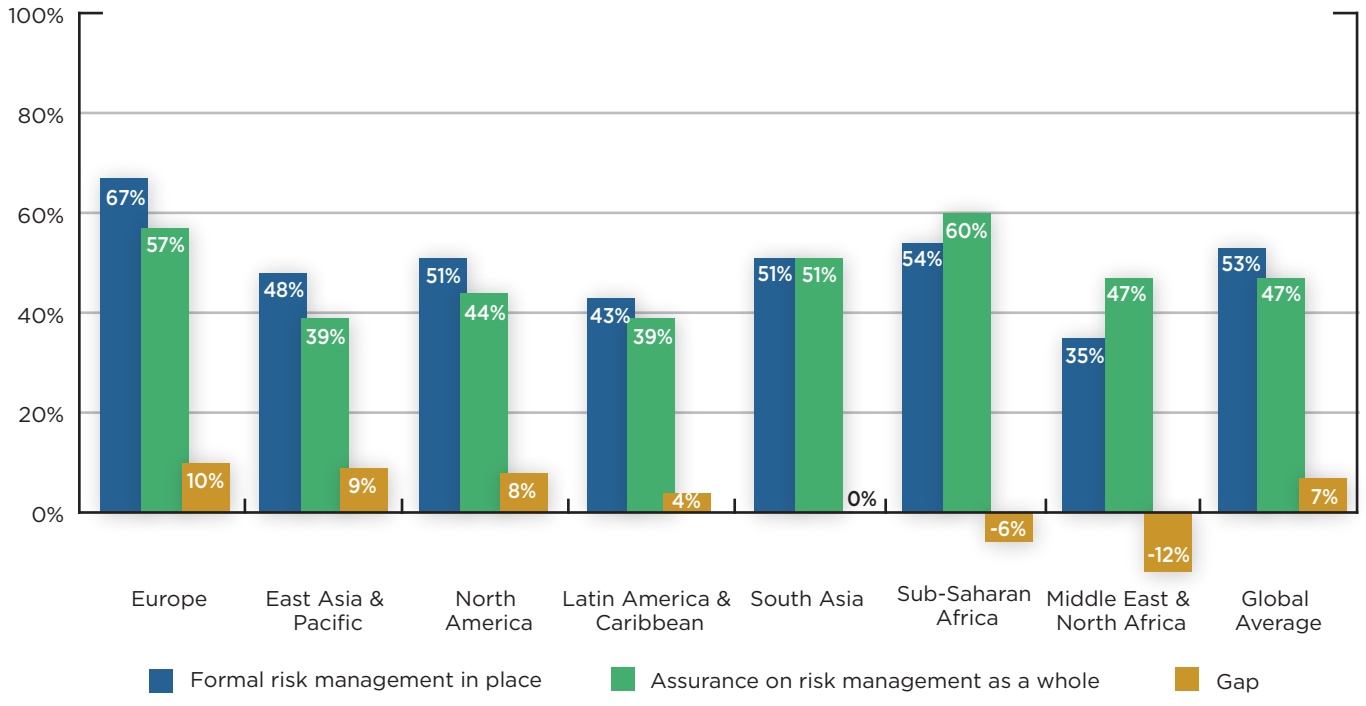
When providing risk management assurance, ensure the criteria for such assurance are well understood.

Gap Analysis by Region

A different way to look at the data is to compare the percentages of companies that have formal risk management (chapter 1) to those that provide assurance on risk management. Because both questions seem to be influenced by regulation, one might hypothesize that there would be some correlation between the two. However, analysis of the gaps between the two survey questions does not necessarily support that hypothesis.

The first gaps we will look at are based on world region (see **exhibit 12**). Recall that globally, 53% indicate they have formal risk management in place (blue bar) and 47% indicate they provide assurance on risk management as a whole (green bar), resulting in a 7% gap (gold bar). Looking at these percentages by region shows some of the gaps are larger than 7%, indicating assurance has not caught up to the level of formal risk management implementation. However, it is also notable that assurance is higher in Sub-Saharan Africa and Middle East & North Africa than formal risk management (which is why the gap goes to negative numbers instead of positive). It would be interesting to understand how such assurance is provided when risk management is not formal. Stating that differently, risk management assurance should be based on recognized and sound criteria, which could be difficult to establish without formal risk management in place.

Exhibit 12 Gap Between Formal Risk Management and Assurance on Risk Management (Region View)



Note: Q60: What areas of responsibility does internal audit have related to risk at your organization? (Choose all that apply.) *n* = 11,935. Q58: What is your organization's level of development for its risk management processes? CAEs only. *n* = 2,675.

KEY ACTION 6

When conducting a risk-based audit, link the scope and results to specific business risks.

> *"Latin America is lower than other parts of the world in providing risk management assurance, as many internal audit functions still follow a more traditional audit approach. However, in the upcoming years, I believe internal auditors in the region will expand their role to provide more assurance on risk management."*
>
> —Nahun Frett, Vice President of Internal Audit, Central Romana Corporation, Ltd., La Romana, Dominican Republic

Gap Analysis by Industry

Looking at the gaps by industry also provides some interesting variances (see **exhibit 13**). First, it is important to note that there were no industries with negative gaps. Second, two of the industries with the highest level of formal risk management—finance and insurance and utilities (see **exhibit 3**) —have two of the largest gaps, well above the global average. However, the other two industries with large gaps—construction and wholesale trade—have formal risk management averages lower than the global average of 53%. While there do not appear to be any consistent reasons for large gaps between formal risk management and assurance on risk management, the existence of such gaps reinforces that internal audit functions have notable opportunities to increase their assurance on risk management as a whole.

Assurance on Individual Risks

Another choice for this survey question was "provide assurance on individual risks." With risk-based auditing being so prevalent around the world, it is surprising that only 44% of respondents indicate that they provide such assurance (see **exhibit 10)**. The variations among different regions, industries, and company sizes show similar patterns as before, although the variations are smaller than with the other survey questions.

Advice and Consulting on Risk

A third option for this survey question was "provide advice and consulting on risk management activities." While a higher percentage chose this option (57%), the variations among the different

Exhibit 13 Gap Between Formal Risk Management and Assurance on Risk Management (Industry View)

Utilities	17%
Construction	16%
Wholesale trade	14%
Finance and insurance	13%
Public administration	10%
Real estate and rental and leasing	9%
Professional, scientific, and technical services	8%
Health care and social assistance	7%
Transportation and warehousing	5%
Manufacturing	5%
Information	4%
Mining, quarrying, and oil and gas extraction	3%
Retail trade	2%
Other	1%
Educational services	1%
Other services (except public administration)	1%
Average	7%

Note: Q60: What areas of responsibility does internal audit have related to risk at your organization? (Choose all that apply.) *n* = 11,935. Q58: What is your organization's level of development for its risk management processes? CAEs only. *n* = 2,675.

demographic groups are not as large. Once again, since one might expect advice to be common among internal audit activities performing risk-based auditing, it is surprising that the response percentages are not higher. It is possible that some respondents view assurance on individual risks and advice as subsets of providing assurance on risk management as a whole, but it is also possible that these percentages are not higher because internal auditors do not have the skills and experience to provide such assurance and advice. This is explored further in chapter 4.

KEY ACTION 7

Continue to increase the percentage of the audit plan focused on risk management.

2015 Audit Plan Focus

The survey also asked CAEs to indicate what percentage of their 2015 audit plan was comprised of audits for "risk management assurance/effectiveness." On average, 12% of audit plans focus on this area, making it the third-highest risk category in the audit plan (see **exhibit 14**).

There are strong signs that the focus on risk management is increasing. In the 2012 Pulse of the Profession survey, respondents indicated they expected to spend 5% of their upcoming plan on risk management effectiveness. In 2013 and in 2014, that number increased to 7%. By 2015, it was at 12%.*

Overall, these results indicate that, while internal auditors are providing assurance and advice as indicated in the previous questions, they are not devoting a large part of their audit plan directly to such assurance and advice. However, it is reasonable to assume time spent in

* The Global Pulse of the Profession Reports (Altamonte Springs, FL: The IIA Audit Executive Center, 2012, 2013, and 2014).

Exhibit 14 Audit Plan Categories for 2015

Operational	24.5%
Compliance/regulatory	15.0%
Risk management assurance/effectiveness	12.0%
Strategic business risks	10.8%
Information technology (IT), not covered in other audits	8.3%
General financial	6.7%
Corporate governance	6.2%
Fraud not covered in other audits	3.5%
Other (in particular, requests, training, etc.)	3.3%
Cost/expense reduction or containment	3.2%
Sarbanes-Oxley testing or support (United States only)	2.8%
Third-party relationships	2.4%
Crisis management	1.2%

Note: Q49: What percentage of your 2015 audit plan is made up of the following general categories of risk? CAEs only. *n* = 2,712.

other areas is still risk-based, so the low percentage devoted to risk management assurance/effectiveness may not be that alarming.

Also of note is that, regionally, North America is notably below other regions of the world (see **exhibit 15**). However, that is primarily driven by the time spent on Sarbanes-Oxley testing in the United States (10.2%). While Sarbanes-Oxley testing focuses only on financial reporting risks, it is reasonable to consider that it also provides risk management assurance.

Combined Assurance

Another relevant topic related to assurance pertains to combined assurance, which is a coordinated effort to combine assurance from multiple internal assurance functions. It can be a key enabler for providing assurance on risk management as a whole because such assurance would come with assistance from other areas. However, overall only 1 out of 4 respondents have implemented combined assurance. Specifically, 19% indicate that their organization has implemented a

Exhibit 15 Audit Plan Categories for 2015 (Region View)

	South Asia	Europe	Sub-Saharan Africa	East Asia & Pacific	Latin America & Caribbean	Middle East & North Africa	North America
Operational	25.9%	24.4%	24.5%	24.7%	22.9%	26.4%	24.9%
Compliance/regulatory	12.9%	14.3%	11.3%	20.0%	14.4%	9.2%	14.6%
Risk management assurance/effectiveness	15.9%	14.2%	13.0%	12.5%	12.4%	11.4%	8.1%
Strategic business risks	10.3%	10.9%	13.6%	7.6%	17.2%	12.1%	8.2%
Information technology (IT), not covered in other audits	7.2%	8.2%	8.3%	4.7%	8.5%	9.4%	11.5%
General financial	8.4%	6.3%	8.3%	7.0%	5.6%	7.8%	6.5%
Corporate governance	6.7%	6.9%	6.9%	8.1%	5.0%	7.1%	3.7%
Fraud not covered in other audits	3.7%	4.0%	3.5%	3.2%	4.4%	3.7%	2.5%
Other (in particular, requests, training, etc.)	1.4%	3.3%	3.3%	2.8%	3.6%	2.2%	4.2%
Cost/expense reduction or containment	5.0%	3.2%	3.4%	4.5%	1.7%	5.9%	1.9%
Sarbanes-Oxley testing or support (United States only)	0.2%	0.6%	0.6%	0.8%	1.7%	0.4%	10.2%
Third-party relationships	2.0%	2.7%	1.8%	2.0%	1.8%	2.0%	3.1%
Crisis management	0.5%	1.1%	1.4%	1.9%	0.8%	2.3%	0.7%

Note: Q49: What percentage of your 2015 audit plan is made up of the following general categories of risk? CAEs only. *n* = 2,712.

KEY ACTION 8

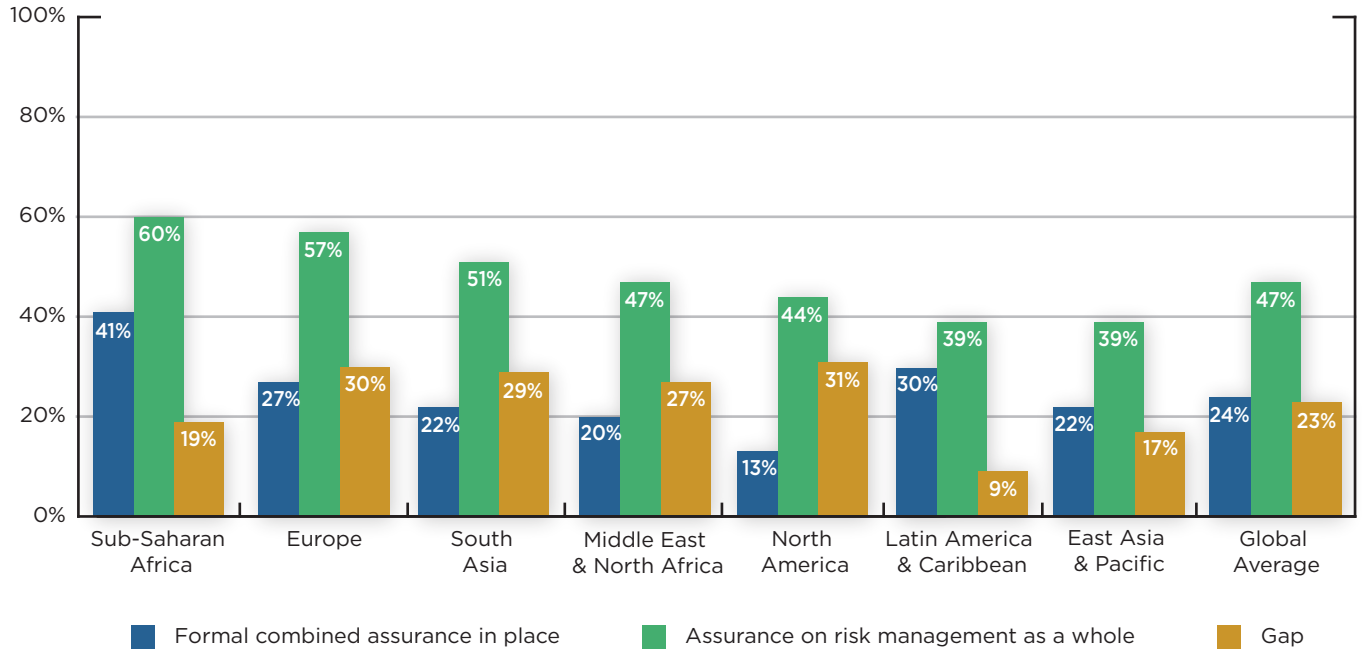
Explore ways to integrate assurance with other internal assurance providers; combined and integrated assurance can be more effective and efficient.

formal combined assurance model, and another 5% indicate that the model is in place but not yet approved by the board. It is interesting that in the three lines of defense discussion in chapter 2, survey results show that 66% of respondents coordinate and share information with the ERM function, but this must be informal coordination and sharing because a much smaller percentage have implemented formal combined assurance. (For more in-depth analysis of combined assurance, please see the CBOK report titled *Combined Assurance: One Language, One Voice, One View*.)

There are predictable differences in the answers to this question as seen for other questions; that is, larger and more regulated companies show higher percentages that have implemented formal combined assurance.

It is interesting to compare regionally the percentage of companies that have formal combined assurance in place against the assurance on risk management as a whole (see **exhibit 16**). In every region, assurance on risk management as a whole (green bars) is consistently higher than the implementation of combined assurance (navy bars), which is to be expected because combined assurance is still an evolving practice. In those regions where combined assurance is relatively high, it is likely that the regulatory climate is an influence. For example, Sub-Saharan Africa has the highest implementation of combined assurance (41%), likely due to the influence of

Exhibit 16 Gap Between Formal Combined Assurance and Assurance on Risk Management (Region View)



Note: Q60: What areas of responsibility does internal audit have related to risk at your organization? (Choose all that apply.) *n* = 11,779. Q61: Has your organization implemented a formal combined assurance model? *n* = 10,417.

> *"There is an increasing trend to segregate the assurance functions, so I do not expect to see an increase in combined assurance in this region (Middle East & North Africa). Integrated assurance has not established a foothold in the region, and I do not anticipate that will change in the near future."*
>
> —Tom Totton, General Manager Internal Audit, Bankmuscat, Sultanate of Oman

governance regulations in South Africa, where the King Report on Corporate Governance (King III) requires a combined assurance model. Surprisingly, combined assurance is next highest in Latin America & Caribbean, which seems to run counter to the responses to other questions. The largest gaps (gold bars) are in North America (31%) and Europe (30%). The European gap is probably due to the implementation of combined assurance not yet catching up with the overall higher level of assurance. However, in North America, the gap simply reflects the very low level of combined assurance (13%). These results clearly show that there are significant opportunities around the world to advance combined assurance models.

One final observation related to combined assurance is that only 14% of CAEs indicate their organizations have implemented a formal combined assurance model, while 24% of directors and senior managers, 22% of managers, and 19% of staff answered "yes" to that question. Those differences are too large to attribute to differences between the companies for which they work. More likely, CAEs are in a better position to judge what formal combined assurance really looks like, while others in internal audit thought some level of assurance by another activity justified their response.

4 Risk Approaches and Competencies

KEY ACTION 9

Periodically discuss with management the key risk areas to ensure internal audit's focus aligns with that of management.

This chapter explores other CBOK questions that provide additional insights into the overall question, "Who owns risk?" Specifically, questions cover how executives perceive risk management as a top risk area versus CAEs, sources of risk assessment information, and risk proficiencies of internal auditors. These insights will help internal auditors do a better job of delivering risk-based services.

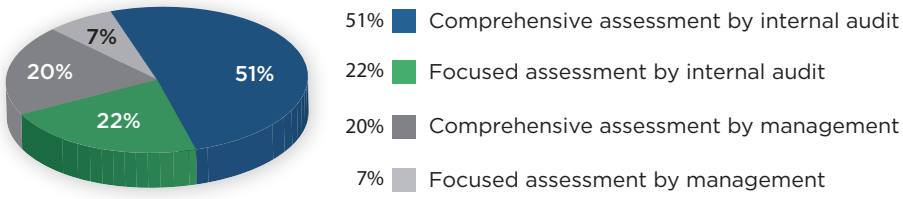
Top Risk Areas

When asked to identify the top five risks on which your *executive management* is focusing the greatest level of attention in 2015, CAEs chose "risk management assurance/effectiveness" 41% of the time. But when asked the same question about the top five risks on which *internal audit* is focusing the greatest attention, CAEs chose it 58% of the time (Q65 and Q66, n = 2,753). Why the difference between what CAEs believe executive management feels deserves a lot of attention versus what internal audit believes deserves attention? One can only hypothesize the answer to that question, but it likely indicates that executive management and CAEs do not spend enough time discussing which areas of risk are most important to the organization and where assurance is most valuable. CAEs may have a better understanding of the value of risk management assurance and need to educate executive management on that value.

Risk Assessment Sources

Risk assessment has been an integral part of risk-based auditing for years, but it was very interesting to discover how internal auditors obtain the risk assessment information they use as a foundation for their activities (see **exhibit 17**). About half the

Exhibit 17 Type of Risk Assessment Relied upon by Internal Audit



Note: Q41: What kind of risk assessment does internal audit rely upon at your organization? CAEs only. n = 2,907.

KEY ACTION 10

Work with risk-related functions to ensure appropriate leveraging and reliance on risk assessment efforts by all such functions.

KEY ACTION 11

Update the risk assessment at the speed of risk, not based on the turning of a calendar page.

CAEs indicate that internal audit does a comprehensive risk assessment while another 22% say their internal audit department conducts focused risk assessments. That means the remaining 27% rely on management's risk assessments (either comprehensive or focused). When comparing this data to the question in chapter 2 (focusing on the relationship between internal audit and ERM), this raises a key question: why do two-thirds of respondents indicate internal audit and risk management are separate functions but they coordinate and share knowledge, yet internal audit relies on management for risk assessment information only a quarter of the time? One might assume that the risk management function must be relying on internal audit's risk assessment, but that seems odd for a risk management function to abdicate that important risk responsibility. It is also possible that risk management does conduct its own risk assessment, but internal audit prefers to rely on its own risk assessment. Either way, there appears to be an opportunity to enhance the collaboration between internal audit and ERM.

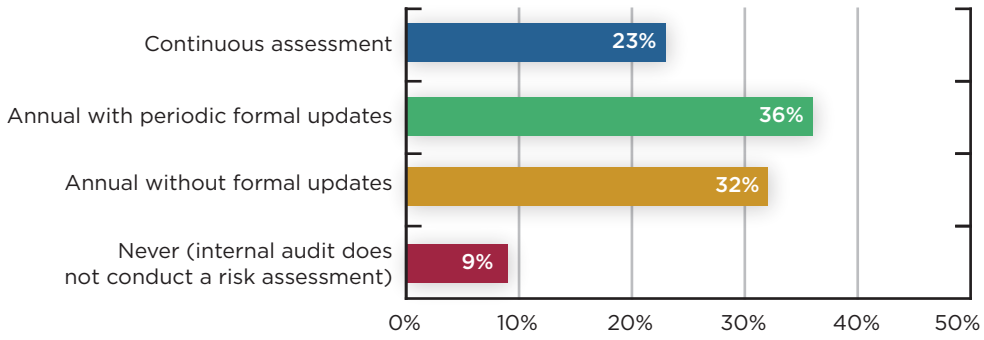
Risk Assessment Frequency

When asked about the frequency of risk assessments, 23% of CAEs say that risk assessment is continuous, and another 36% say they do an annual risk assessment with formal updates (see **exhibit 18**). The remaining 41% are either not considering how risks change within the year or are doing so informally. Given how quickly the world changes and, as a result, a company's risk profile changes, the 41% who are not formally updating their risk assessment in some way may not be optimizing the value of their internal audit function. This should be discussed with their key stakeholders, who may assume emerging and changing risks are being considered by internal audit in a timely manner, when in reality they are not.

Risk Data Archives

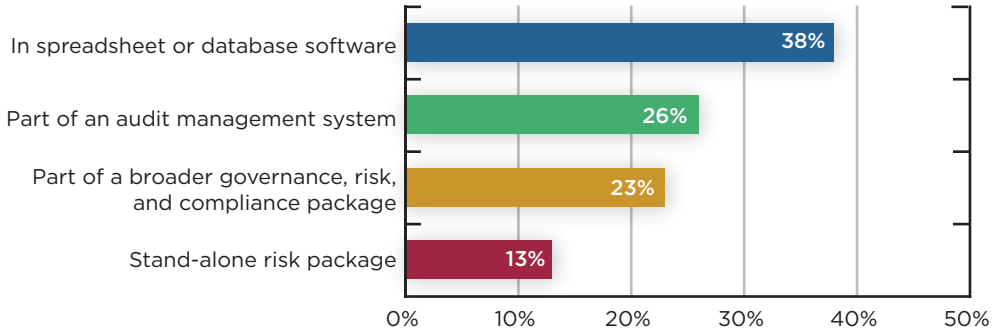
Maintaining a large volume of risk assessment data in an ever-changing world can be challenging; therefore, the survey also asked CAEs how their risk assessment is maintained. The respondents could choose from four technology options. Because most audit management systems

Exhibit 18 Frequency of Risk Assessment



Note: Q42: How frequently does internal audit conduct a risk assessment? CAEs only. *n* = 2,986.

Exhibit 19 Technology Used to Maintain Risk Assessments



Note: Q43: How is your risk assessment maintained? CAEs only. *n* = 2,667.

KEY ACTION 12

While requests from management should typically be considered for an audit plan, be cautious to ensure such requests do not divert valuable internal audit resources from higher-risk areas.

can handle changes to the risk components, it is somewhat encouraging that 62% of respondents use software designed to manage risk information (see **exhibit 19**). The 38% who continue to use spreadsheet or database software may find the need to evaluate the benefits of using software products designed to deal with such risk information.

Audit Plans Based on Risk

Finally, 85% of respondents indicate they use a risk-based methodology as a resource to establish their audit plan (the #1 response) (see **exhibit 20**). While there is some variability across regions, industries, and company sizes, all had "risk-based methodology" as the #1 or #2 resource for their audit plans. For the few

Exhibit 20 Resources Used to Establish the Audit Plan

A risk-based methodology	85%
Requests from management	72%
Analysis of the organization's strategy or business objectives	64%
Consultations with divisional or business heads	62%
Compliance/regulatory requirements	62%
The previous year's audit plan	61%
Requests from the audit committee	56%
Consultations with external auditors	26%
Requests from external auditors	19%
Other	6%

Note: Q48: What resources do you use to establish your audit plan? (Choose all that apply.) CAEs only. *n* = 3,040.

KEY ACTION 13

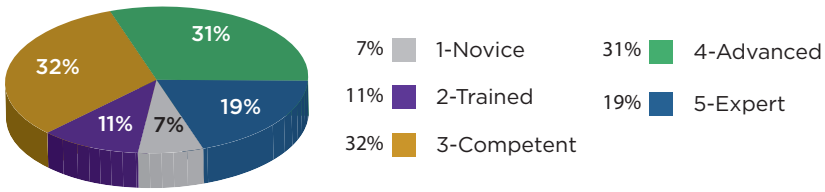
Continue to grow internal audit capabilities around risk to ensure internal audit functions can meet the changing stakeholder expectations of the future in a world that increasingly becomes more complex and risky.

that ranked it #2, requests from management was the #1 choice. This confirms that risk is the primary foundation for internal audit activities around the world.

Risk Competency Levels

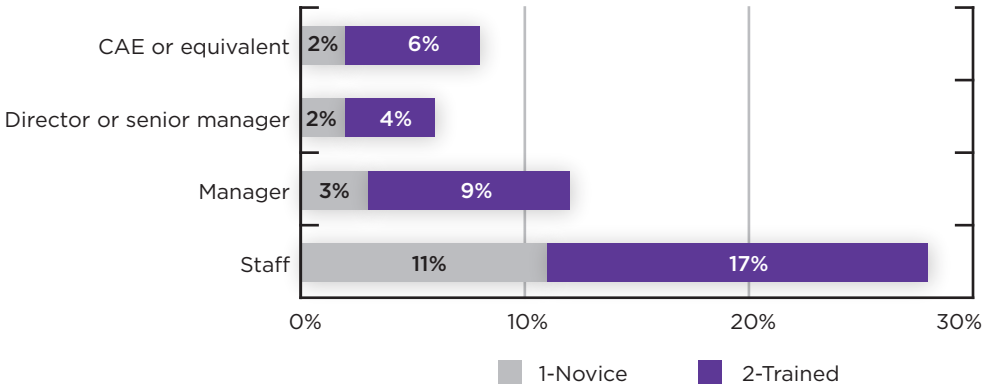
To execute a risk-based audit methodology, internal auditors must have a certain level of competence related to risk. When asked to describe their level of proficiency related to applying the organization's risk framework in audit engagements (see **exhibit 21**), most respondents assess themselves as competent (32%), advanced (31%), or expert (19%). While the combined total of 82% seems to correlate closely to the 85% of respondents who employ a risk-based methodology, one would have hoped that respondents assessing themselves as at least competent would have approached 100%. However, a majority of the novice and trained assessments came from staff (see **exhibit 22)**, so perhaps it is not surprising that less experienced people do not yet consider themselves competent with regard to risk.

Exhibit 21 Risk Proficiency Self-Assessments



Note: Q81: Estimate your proficiency for each competency using the following scale: 1-Novice; 2-Trained; 3-Competent; 4-Advanced; 5-Expert. Topic: Apply the organization's risk framework in audit engagements. *n* = 10,842.

Exhibit 22 Risk Proficiency Self-Assessment at Novice/Trained



Note: Q81: Estimate your proficiency for each competency using the following scale: 1-Novice; 2-Trained; 3-Competent; 4-Advanced; 5-Expert. Topic: Apply the organization's risk framework in audit engagements. *n* = 10,518.

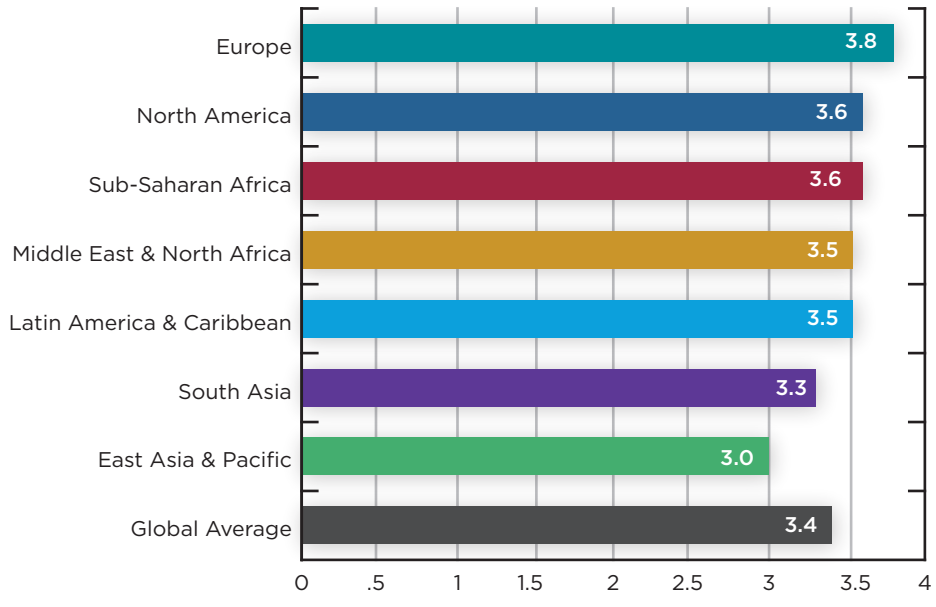
> *The trend in Sub-Saharan Africa to become more competent around risk is consistent with the needs and expectations of stakeholders in the region. The downside is that so many organizations are poaching staff from internal audit functions as they implement formal risk management.*
>
> —Andy Chitete, Senior Risk Manager, Electrical Supply Corporation of Malawi (ESCOM), Blantyre City, Malawi

It is also interesting to note that there are differences in risk proficiency between the various regions around the world (see **exhibit 23**), likely reflecting the different maturity levels related to risk within these regions, as discussed throughout this report. This chart shows the average perceived proficiency in applying the organization's risk management framework, where those who assessed themselves as expert received a score of 5, advanced 4, competent 3, trained 2, and novice 1. Europe led the regions, while East Asia & Pacific was the lowest. These results are somewhat consistent with the results from chapter 1 related to the implementation of formal risk management.

Such differences are smaller among the various industries (see **exhibit 24**). It is interesting that all other risk-related CBOK data indicates that finance and insurance companies are typically more mature related to risk topics, presumably because of the heavier regulations on those industries. However, for this question, they are close to the global average and in line with most other industries.

It is important to note that the 2010 CBOK study included a report titled *Core Competencies for Today's Internal Auditor*. Almost 60% of respondents to that year's survey indicated that ERM was a very important area of knowledge for internal auditors. Additionally, the 2012 and 2013 Pulse of the Profession surveys conducted by The IIA's Audit Executive Center identified risk management assurance as one of the top five skills sought throughout the world. Based on the results of the CBOK 2015 survey, it appears the focus on risk management skills may be paying off.

Exhibit 23 Average Risk Proficiency Self-Assessment (Region View)



Note: Q81: Estimate your proficiency for each competency using the following scale: 1-Novice; 2-Trained; 3-Competent; 4-Advanced; 5-Expert. Topic: Apply the organization's risk framework in audit engagements. *n* = 10,711.

Exhibit 24 **Average Risk Proficiency Self-Assessment (Industry View)**

Professional, scientific, and technical services	3.6
Health care and social assistance	3.6
Finance and insurance	3.5
Utilities	3.5
Mining, quarrying, and oil and gas extraction	3.5
Retail trade	3.5
Real estate and rental and leasing	3.5
Public administration	3.4
Other services (except public administration)	3.4
Transportation and warehousing	3.4
Educational services	3.4
Other	3.4
Manufacturing	3.3
Construction	3.2
Wholesale trade	3.2
Information	3.1
Average	3.4

Note: Q81: Estimate your proficiency for each competency using the following scale: 1-Novice; 2-Trained; 3-Competent; 4-Advanced; 5-Expert. Topic: Apply the organization's risk framework in audit engagements. *n* = 10,571.

Conclusion

Risk continues to be the foundation of internal auditing around the world. While the risk responsibilities of other functions within the organization are growing, internal audit continues to have an important role around risk.

Increases in regulation seemed to fuel the growth in formal risk management after the global financial crisis. However, while the growth in risk management is continuing, the pace of growth may be slowing down.

The trend to separate risk management from internal audit is continuing, although there remain vulnerabilities to blurring the second and third lines of defense. Internal audit is providing more assurance over risk management as a whole, although such assurance still lags behind the level of formal risk management processes in place. Additionally, implementation of a combined assurance model remains relatively low, indicating that the efficiency of risk management assurance has not yet been optimized.

CAEs perceive the importance of risk management assurance higher than does management. This indicates there are opportunities to work closer with key stakeholders on expectations around risk management assurance. Also, there may be opportunities for internal audit and risk management to better coordinate the risk assessment activities to ensure each appropriately leverages the knowledge of the other. Finally, risk competencies among internal auditors also seem to be growing, which helps the profession confront the growing expectations from stakeholders.

However, there are many areas where internal audit may not be advancing as much as will be needed in a world growing more complex and risky all the time. Throughout this report, key actions are identified for CAEs and internal auditors to consider. By focusing on these key actions, internal audit functions will be better positioned to meet the growing stakeholder demands around risk.

Risk Management Recommendations

1. Be advocates for the advancement of formal risk management processes, regardless of industry.
2. Seek opportunities to help expedite the implementation of formal risk management, and sustain it when it is already in place.
3. Work with management and other internal assurance providers to ensure clarity of roles within the three lines of defense.

4. Strive to provide assurance on risk management as a whole, not just on individual risks.
5. When providing risk management assurance, ensure the criteria for such assurance are well understood.
6. When conducting a risk-based audit, link the scope and results to specific business risks.
7. Continue to increase the percentage of the audit plan focused on risk management.
8. Explore ways to integrate assurance with other internal assurance providers; combined and integrated assurance can be more effective and efficient.
9. Periodically discuss with management the key risk areas to ensure internal audit's focus aligns with that of management.
10. Work with risk-related functions to ensure appropriate leveraging and reliance on risk assessment efforts by all such functions.
11. Update the risk assessment at the speed of risk, not based on the turning of a calendar page.
12. While requests from management should typically be considered for an audit plan, be cautious to ensure such requests do not divert valuable internal audit resources from higher-risk areas.
13. Continue to grow internal audit capabilities around risk to ensure internal audit functions can meet the changing stakeholder expectations of the future in a world that increasingly becomes more complex and risky.

About the Author

Paul J. Sobel, CIA, QIAL, CRMA, is vice president/chief audit executive for Georgia-Pacific, LLC, a privately owned forest and consumer products company based in Atlanta, Georgia. He previously served as the CAE for three public companies, where his responsibilities included leading the global internal audit efforts, as well as consulting on each company's ERM, compliance, and internal controls programs.

Sobel has published three books, the first of which is titled *Auditor's Risk Management Guide: Integrating Auditing and ERM.* He co-authored The IIARF textbook titled *Internal Auditing: Assurance & Consulting Services*, and more recently co-authored a book focused on ERM titled *Enterprise Risk Management: Achieving and Sustaining Success*.

He has held may IIA volunteer roles, including chairman of the Board of Directors in 2013–2014. He is currently one of The IIA's representatives on the COSO ERM Advisory Council and also served on the Public Company Accounting Oversight Board's (PCAOB's) Standing Advisory Group. In 2012, he was recognized in *Treasury & Risk Magazine*'s list of 100 Most Influential People in Finance.

About the Project Team

CBOK Development Team

CBOK Co-Chairs:
Dick Anderson (United States)
Jean Coroller (France)
Practitioner Survey Subcommittee Chair:
Michael Parkinson (Australia)
IIARF Vice President: Bonnie Ulmer
Primary Data Analyst: Dr. Po-ju Chen
Content Developer: Deborah Poulalion
Project Managers: Selma Kuurstra and Kayla Manning
Senior Editor: Lee Ann Campbell

Report Review Committee

Sezer Bozkus (Turkey)
John Brackett (United States)
John McLaughlin (United States)
Michael Parkinson (Australia)
Beatriz Sanz-Redrado (Belgium)
Maritza Villanueva (El Salvador)

Your Donation Dollars at Work

CBOK reports are available free to the public thanks to generous contributions from individuals, organizations, IIA chapters, and IIA institutes around the world.

Donate to CBOK

www.theiia.org/goto/CBOK

About The IIA Research Foundation

CBOK is administered through The IIA Research Foundation (IIARF), which has provided groundbreaking research for the internal audit profession for the past four decades. Through initiatives that explore current issues, emerging trends, and future needs, The IIARF has been a driving force behind the evolution and advancement of the profession.

Limit of Liability

The IIARF publishes this document for information and educational purposes only. IIARF does not provide legal or accounting advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

Contact Us

The Institute of Internal Auditors Global Headquarters
247 Maitland Avenue
Altamonte Springs, Florida 32701-4201, USA