Auditing Strategic Risks

Practical Insights from Internal Audit Leaders

A CBOK Stakeholder Report

J. Michael Joyce Jr.
CIA, CPA, CRMA

protiviti®
Face the Future with Confidence

The IIA Research Foundation

CBOK
The Global Internal Audit Common Body of Knowledge

STAKEHOLDER STUDY FACTS

Survey participants	1,124
Interview participants	112
Countries	23
Languages	13

STAKEHOLDER POSITIONS REPRESENTED

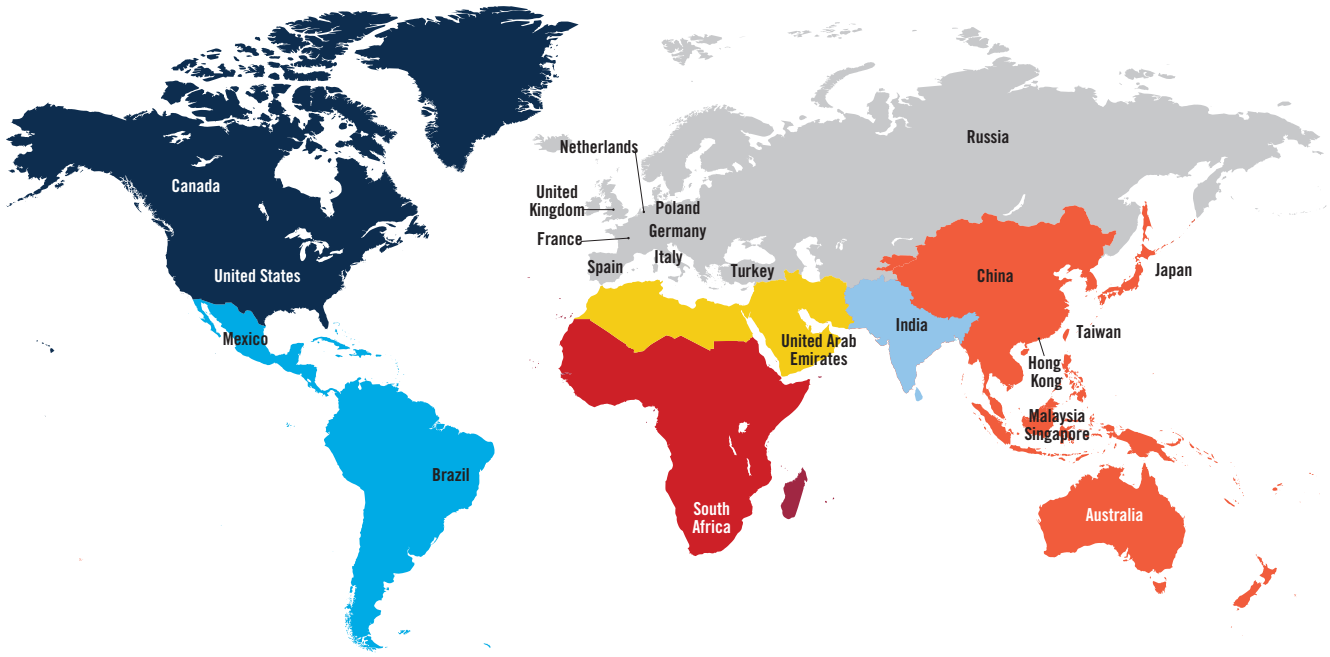
Board member	34%
Chief executive officer (CEO)	15%
Chief financial officer (CFO)	18%
Other C-suite	33%

About CBOK

The Global Internal Audit Common Body of Knowledge (CBOK) is the world's largest ongoing study of the internal audit profession. The current CBOK study has two major components: practitioner and stakeholder. The practitioner study encompasses reports that explore a variety of internal audit practices. To complement this information, the stakeholder study seeks out perspectives from stakeholders about internal audit performance. Surveys, interviews, and data analysis for the stakeholder project were conducted by Protiviti in partnership with IIA institutes around the world. Stakeholder reports focus on identifying leading practices that can improve internal audit effectiveness.

CBOK reports are available free of charge thanks to generous contributions and support from individuals, organizations, IIA chapters, and IIA institutes worldwide. Practitioner and stakeholder reports are available for download at the CBOK Resource Exchange (www.theiia.org/goto/CBOK). Stakeholder reports are also available at the Protiviti website (www.protiviti.com).

CBOK 2015 Stakeholder Study: Participants from 23 Countries



Note: Twenty-three countries participated with the Internal Audit Foundation, formerly the IIA Research Foundation (IIARF), and Protiviti to distribute surveys and interview questionnaires to stakeholders in their region from July 2015 to February 2016. Partially completed surveys were included in the analysis as long as demographic questions were complete. Questions in CBOK reports are referenced as Q1, Q2, and so on. The colors on the map show the seven global regions (based on World Bank categories) used for CBOK studies.

About the CBOK 2015 Global Stakeholder Study

This report is part of the Internal Audit Foundation's 2015 Common Body of Knowledge (CBOK) Global Stakeholder Study. One of the key findings in this study is that nearly two-thirds (64 percent) of stakeholders – board members, CEOs, CFOs, CIOs, CROs and more – want internal audit to be more active in strategic risks. As a follow-up initiative in this ongoing study, chief audit executives (CAEs) from across multiple industries were interviewed to gain insight on how they are more active in strategic risks focused on three common areas – cyber-security, IT projects, and capital projects. The insights of these audit leaders, whom we cite throughout our report without attribution in exchange for their candid feedback and views, inform our discussion.

Contents

Introduction: Familiar and Fascinating Insights into Auditing Strategic Risks

> *"We keep an eye on the assumptions – those that initially drove the strategic initiative and those that continue to drive the initiative as it progresses. Do those assumptions remain relevant?"*

The insights on leading practices shared by CAEs are by turns familiar and fascinating when these leaders open up about how their internal audit functions work with management and the board to address three specific areas of strategic risk for their organizations: cybersecurity, IT projects, and capital projects.

The familiarity stems from the risk-based approach of audit leaders for these strategic risk areas, as well as what they say about the underlying enablers of effective "strategic auditing" – an activity that more board members, CEOs, CFOs, and other C-suite executives are encouraging internal audit to perform. CAEs consistently point to the value of internal audit's early involvement in strategic initiatives, its risk-based auditing approach, internal audit's credibility in the eyes of business partners, and the function's capacity to thrive in an advisory manner. These critical building blocks have existed within top-performing audit functions for some time.

Two other takeaways emerged from this dialogue, as well, that are more unexpected. First, internal audit functions are making significant progress in how they audit and address strategic risks by leveraging a broad range of approaches (as we review in the cybersecurity, IT projects, and capital projects sections). Second, leading internal audit functions work diligently, and inventively, to validate their seat at the decision-making table, their function's credibility, and their advisory role through specific enablers (which are summarized in the final part of this report).

The interviews conducted served a dual purpose: by describing how they address strategic risks, leading audit executives highlighted ways they nurture the function's role as a strategic partner to the business, without jeopardizing, first and foremost, their focus on compliance and assurance responsibilities.

Cybersecurity Does Not Exist in a Vacuum

"Cybersecurity has to work like all the systems and parts of a human body work together to defend against threats and to make it work efficiently. It's not a stand-alone process. There is not a single element of our company that does not affect cybersecurity."

One CAE responded immediately when asked how auditing a massive capital project underway in a war-torn region compared to auditing cybersecurity: "Our capital project is not as complex and not as daunting."

Audit committees are pressing for updates on the organization's ability to address cybersecurity, an overwhelming strategic risk. CAEs are responding through multiple avenues such as sharpening their view of organizational cybersecurity through formal risk assessments and first-hand involvement in cybersecurity steering committees and exercises; increasing and expanding cybersecurity-related areas in audit plans; and aligning their risk management activities with IT, information security, and enterprise risk management (ERM) functions.

Overall, the CAEs interviewed cited the following activities and best practices most frequently when describing what drives their effectiveness in auditing cybersecurity:

- **Engage with those who set and shape cybersecurity strategy:** While emphasizing that their functions conducted identity management, patch management, and many other forms of cybersecurity auditing long before the term "cybersecurity" took on its current meaning and import, audit leaders report that they have more recently sought out advisory roles with committees responsible for setting and strengthening organizational cybersecurity strategies and capabilities. Another option to consider, as one CAE noted: "Work with the audit committee to create a dedicated cybersecurity subcommittee, reporting to the audit committee, that consists of outside experts who can provide relevant input on critical and timely cybersecurity issues."

Strategic Risk Auditing Best Practices:

CYBERSECURITY

- *Engage with those who set and shape cybersecurity strategy.*
- *Clarify and coordinate with others on cybersecurity risk responsibilities.*
- *Conduct a formal risk assessment.*
- *Advise on cybersecurity frameworks, standards, and guidance.*
- *Assess cyber resiliency.*
- *Learn continuously.*
- *Own the cybersecurity skills and expertise challenge.*

- **Clarify and coordinate with others on cybersecurity risk responsibilities:** CAEs work closely with their partners in the IT, information security and ERM groups to identify the specific cybersecurity activities each group is conducting. This coordination helps synchronize all efforts in an organization regarding cybersecurity, while reinforcing internal audit's role in providing objective, independent assurance on cybersecurity risk. One CAE conducts, with his CIO, presentations of cybersecurity risks to the audit committee to demonstrate that "we're working in a coordinated manner based on a common risk-evaluation approach."

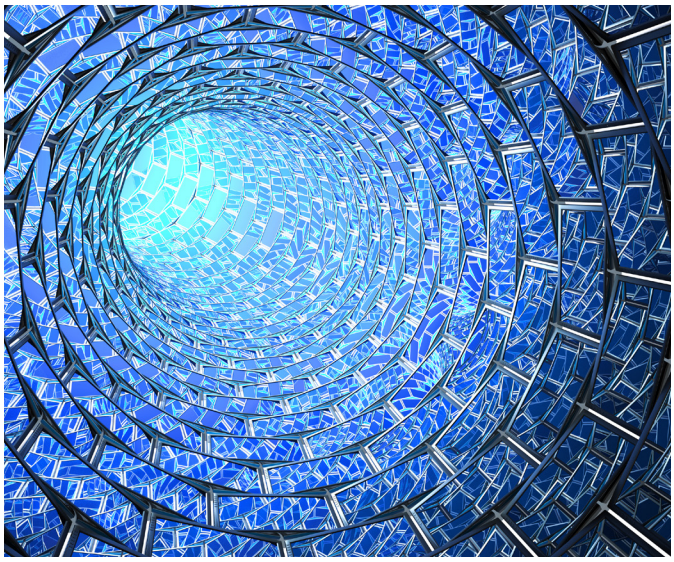
- **Conduct a formal risk assessment:** Formal risk assessments – whether performed by internal audit or a third-party expert – are a crucial part of a cybersecurity regimen. These evaluations identify gaps, clarify improvement and remediation priorities (e.g., addressing a major increase in phishing emails), help determine cybersecurity facets of the audit plan, influence cybersecurity advisory work, and help the organization align on its cybersecurity risks and improvement objectives.

- **Advise on cybersecurity frameworks, standards, and guidance:** Every CAE mentioned one or more sets of cybersecurity standards that their organization uses – and almost always customizes – to help structure the overall cybersecurity program and related assurance activities. These standards include the NIST Cybersecurity Framework, ERM, HITRUST, COBIT, ISO, The IIA's Global Technology Audit Guide (GTAG): Assessing Cybersecurity Risk: Roles of the Three Lines of Defense, CSC20, FFIEC, and more. One CAE who applauds the ERM framework for numerous benefits – including the consistency, transparency, and board exposure to cybersecurity risk it enables – also emphasizes that the framework "may not be sufficient in India, Australia, or other geographies, for example … where other cybersecurity risk management models are used. We've taken what we believe is best from all of the models and applied them to meet our global needs." CAEs' direct involvement in the discussion and evaluations of each of the potential frameworks, and their advantages and disadvantages, positions internal audit to help their organizations gain the most value from the frameworks.

- **Assess cyber resiliency:** Accepting the fact that, in today's environment, a breach is inevitable, CAEs should assess the organization's ability to respond, communicate, and recover when a breach does occur. Areas to consider include not only business continuity procedures, but also communications and crisis management plans.

- **Learn continuously:** Knowledge – of external threats, emerging standards, new compliance requirements, and even psychological profiling – is a crucial driver of cybersecurity auditing success. "I am a CISSP," noted one CAE, "and I spend a large amount of time studying and researching cybersecurity … [as an example], I want to know exactly how Equifax was breached." This same leader also exhorts his team to understand the mindset of a wide range of stakeholders who could expose, knowingly or unwittingly, his company to a cybersecurity threat. "Internal audit needs to understand a hacker's thought process and methodology," he said. "An internal auditor has to be able to think like an accountant, an investor, a lawyer, a compliance specialist, a salesman, a human resource executive – anyone who might create a risk that exposes the company to a cybersecurity lapse." And part of the function's assurance work relates to the effectiveness of cybersecurity training and awareness conducted throughout the organization.

- **Own the cybersecurity skills and expertise challenge:** Most CAEs confirm that hiring and retaining internal auditors with IT and cybersecurity expertise is a challenge. They address this obstacle via talent management strategies and tactics, including making investments in training and development, using external experts, and working closely with human resources colleagues to design recruiting, performance, and retention incentives.



IT Projects: Scrutinizing Data, Development, and Behaviors

"If people think cybersecurity and IT projects are separate, they're misled."

As more companies go all-in on digital transformation and as more IT systems and applications migrate to the cloud, a larger collection of IT projects of all sizes and scope qualify as strategic risks. As a result, a much wider variety of IT projects and application development activities require auditing scrutiny.

This scrutiny can help the internal audit function, as well. One CAE recalls a major software implementation that concerned his IT auditors because the third party responsible for testing the system did not provide sufficient clarity around its test results. "We stepped forward, and we had the facts to support our assertion that we were not comfortable with the testing results and, therefore, that we were not prepared to provide sign-off," he explains. His team's thorough documentation convinced the company that additional testing was needed prior to the system going live. "That helped us, as a function, to establish our presence," the executive continues. "Since then, the software testing lifecycle has continued to improve."

Similar types of detailed scrutiny and fact-based fortitude figure prominently in the areas audit leaders identify as driving effectiveness in auditing IT projects:

- **Develop a structured, multiphased assessment process:** CAEs stress the value of developing and improving the structured evaluations for each phase of an IT project. Given the growing amount, value, and importance of data involved in new implementations and system conversions, security is frequently identified as a starting point for the project assessment. One CAE explained how her IT audit teams now organize IT project engagements into two groups: one focused on system conversions that involve financial controls and require input from both IT and financial auditors; and a second category that focuses more on traditional IT project management methodology, governance, and efficiency.
- **Remove behavioral barriers:** One CAE detailed how a team of IT auditors discovered numerous instances where IT project teams downplayed, or downright obscured, problems that arose. The internal audit group subsequently revamped its communications with those project teams. "Once we saw that they were unwilling to bring forward important issues, we worked on getting them more comfortable doing so," explained the audit leader. "Regarding the red, yellow, green evaluation system, we started a new mantra: 'Red is not dead.'" The IT audit team also made a clear business case for the benefits of surfacing and fixing problems sooner in the project lifecycle rather than later, when the impacts and costs of small issues can be much greater.

Strategic Risk Auditing Best Practices:

IT PROJECTS

- *Develop a structured, multiphased assessment process.*
- *Remove behavioral barriers.*
- *Create advisory offerings to complement assurance work.*
- *Recognize the need to address Agile development.*

- **Create advisory offerings to complement assurance work:** One IT audit group has developed an advisory offering consisting of the higher-level criteria IT auditors assess when conducting a formal audit of an IT project (for example: Do we have an implementation strategy? Who is our sponsor? Is funding approved? What are the known project risks? What contingency planning is needed?). Once the IT auditors and IT project teams work through the list of questions, the IT auditors provide recommendations, as opposed to formal management action plans. "It's been very well accepted," says the CAE. "Today, they rarely need this service from us because they do this on their own through the steps we documented and shared."

- **Recognize the need to address Agile development:** Many CAEs we talked with are currently determining how to address risks associated with Agile development methodologies that more IT functions are embracing. Although this highly collaborative, iterative, and streamlined software development approach greatly reduces the time it takes to create new applications and indirectly improves organizational agility and speed to market, an Agile methodology poses risk-related challenges. "From an audit perspective, we have to figure out things like requirements traceability, whether development teams are obtaining the correct approvals on design, and more," says an auditing executive. "It can benefit organizations, but it also poses new risks."

Capital Projects: Process Is Everything

"We audit the process, not the person."

CAEs whose functions conduct audits and assessments of large capital projects tend to emphasize the importance of two distinctions. First, they say it is important to differentiate monitoring the health and progress of each capital project, which is management's responsibility, and the assurance that internal audit delivers. Second, leading CAEs distinguish between their work on individual capital projects and the need to assess their organization's overall capital project management capability. The latter can greatly help the former.

CAEs cited the following activities and best practices as particularly helpful in driving the effectiveness of their capital project assurance and advisory work:

- **Get involved early in planning:** While internal audit's early involvement in any strategic initiative is an advantage to the organization, this is particularly the case with, for example, a $500 million, multiyear, ground-up construction project on the other side of the world. This involvement often leads to early-stage risk assessments that focus heavily on project governance structures. One such risk assessment, a CAE reports, resulted in fundamental changes, including to the role of the engineering group, procurement group, and construction contractor (and who filled it), that altered the trajectory of the work.

- **Focus on the underlying rationale for the investment:** Many capital projects take years to reach completion and the assumptions underpinning the decision to make the investment can change over time. As part of capital project audits, one CAE and his team identify which data sources are being used to validate the decision-making assumptions. "We selectively test where it makes sense and where it is practical for us to test those assumptions," he continues. "We ask, 'What facts did you rely on? If you conducted modeling, how do you know the models are accurate? How do you know the formulas have integrity? Is projected return on investment confirmed/validated?'"

- **Deploy specialized expertise:** One CAE recently hired an external construction auditor to conduct a detailed review of the general contractor's invoices on a type of building that the company had never previously constructed. "That investment," he notes, "enabled us to ask technical questions that only someone who had experience with that type of construction project would know to ask." Other leaders hire and retain internal auditors with extensive capital projects and construction experience – they know what issues to look for and possibly challenge as they walk job sites, attend project meetings, and verify status reports.

- **Conduct rigorous, process-focused project reviews:** In most cases, capital project audits are comprehensive and highly manual. Governance assessments determine whether project steering teams are focusing on relevant risks and receiving correct, complete, and timely information. Assessments of completion

Strategic Risk Auditing Best Practices:

CAPITAL PROJECTS

- *Get involved early in planning.*
- *Focus on the underlying rationale for the investment.*
- *Deploy specialized expertise.*
- *Conduct rigorous, process-focused project reviews.*
- *Consult on capital project management improvements.*
- *Perform postmortem audits and reviews.*

progress and budgets require reviews of massive volumes of information – supporting documentation accompanying the general contractor's application for payment tends to be particularly thick. While a rigorous approach is absolutely necessary, CAEs consistently stress the need to make it clear to project managers that the audit is centered on processes as opposed to individuals. Striking this balance requires auditors to translate risk, internal controls, and other auditing nomenclature and perspectives into terms that resonate with time-pressed project managers.

- **Consult on capital project management improvements:** One internal audit function has developed an advisory offering that capital project teams can use at the onset of a new initiative. The service provides guidance on key operational controls, financial controls, and project risks the team should consider, along with fraud-awareness and prevention training related to contractor billing activities. "In this role, our goal is to be a risk adviser and strategic partner without getting in the way of early deadlines and a successful implementation," says the CAE. Another internal audit group participates in a strategic initiative centered on improving the company's capital project management capability and, specifically, how return on investment is measured and monitored. In this organization, the internal audit function's role is to ensure that appropriate controls are built into new processes the team develops.

- **Perform postmortem audits and reviews:** The results of these activities can provide valuable feedback on the validity of original assumptions used to justify the capital project and enhance approaches for future projects, including the possible engagement of internal audit earlier in the project.

Four Enablers Behind Leading Internal Audit Functions

In addition to the specific items identified above, comments and insights from CAEs reveal a number of underlying enablers that are pivotal to the success of strategic auditing activities. These qualities are present in each of the audit functions helmed by the CAEs interviewed.

Four Key Enablers:

1. *Ongoing demonstrations of value*
2. *Access*
3. *Common language*
4. *Participation*

1. Ongoing demonstrations of value: Most CAEs describe an origin story of their internal audit function's acceptance as a strategic assurance and advisory partner to the business. Like flashbacks in a movie that uncover how superheroes gained their otherworldly powers, these descriptions pinpoint the circumstances under which internal audit's actions transformed the way that C-level executives, board members, and process owners view their internal audit function. More notably, internal audit leaders stress that their function's hard-earned reputations must be nurtured and sustained through ongoing demonstrations of value. New leaders and process owners continually join the organization – sooner or later, they seek evidence that internal audit's credibility is warranted.

2. Access: Demonstrations of the internal audit function's value along with the CAE's commitment to ongoing relationship-building grant these leaders important "hall pass" access to board members, C-level executives, and process owners throughout the enterprise. This access translates into valuable knowledge of what is happening throughout the organization and what strategic shifts and initiatives may be on the horizon.

3. Common language: It is striking how many CAEs mentioned the importance of translating the term "internal controls" into terminology that IT functions, the CISO, the capital project manager, and other process owners can understand in their context. "We altered the definition of internal controls," said one audit executive, "to mean those processes that move whoever you are – a plant, a function, a location – toward your goals." CAEs emphasize a need to translate all of the function's work into practical, well-understood terms that hold meaning for stakeholders in their environments.

4. Participation: Leading audit functions tend to be highly active and participatory. They join tabletop incident response activities designed to expose cybersecurity lapses. They spend meaningful time on shop floors and construction sites. "We conduct network penetration testing as part of our audit plan," said one CAE. "That gives us a better grasp of vulnerabilities and how management is addressing them." That information, which the leader shares with the board, helps makes her cybersecurity risk updates more tangible for the audit committee.

Final Thoughts: Assurance Before Advisory

Although CAEs describe an interesting collection of advisory services their functions deliver to help the organization address strategic risks, they also emphasize – in no uncertain terms – that assurance work always comes first.

This anecdote may say it all: After a few weeks on the job, a newly hired senior auditor asked her CAE why the function did not more actively promote its growing collection of advisory services. His response clarified the function's priorities: Rather than lead with advisory services, he explained, "I'd rather have the people that we've done business with on the assurance side, who understand our value, ask us to do advisory services. I think that's how you want to bring customers in."

About the Author

J. Michael Joyce Jr., CIA, CPA, CRMA, FAHM, is the Vice President, Chief Auditor & Compliance Officer for the Blue Cross Blue Shield Association (BCBSA), a national federation of 36 independent, community-based and locally operated Blue Cross and Blue Shield companies. The Blue System is the nation's largest health insurer covering more than 107 million members — one in three of all Americans. Joyce directs the internal audit, national anti-fraud and compliance staff functions for the association. He has 35 years of professional experience and has been with BCBSA since June 1999. He has been an active IIA volunteer since 1989.

About the Internal Audit Foundation

CBOK is administered through the Internal Audit Foundation, 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 Foundation has been a driving force behind the evolution and advancement of the profession. The Foundation may be contacted at 1035 Greenwood Blvd., Suite 401, Lake Mary, Florida 32746, USA.

About Protiviti Inc.

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk, and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

Limit of Liability

The Internal Audit Foundation publishes this document for information and educational purposes only. The Internal Audit Foundation 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.