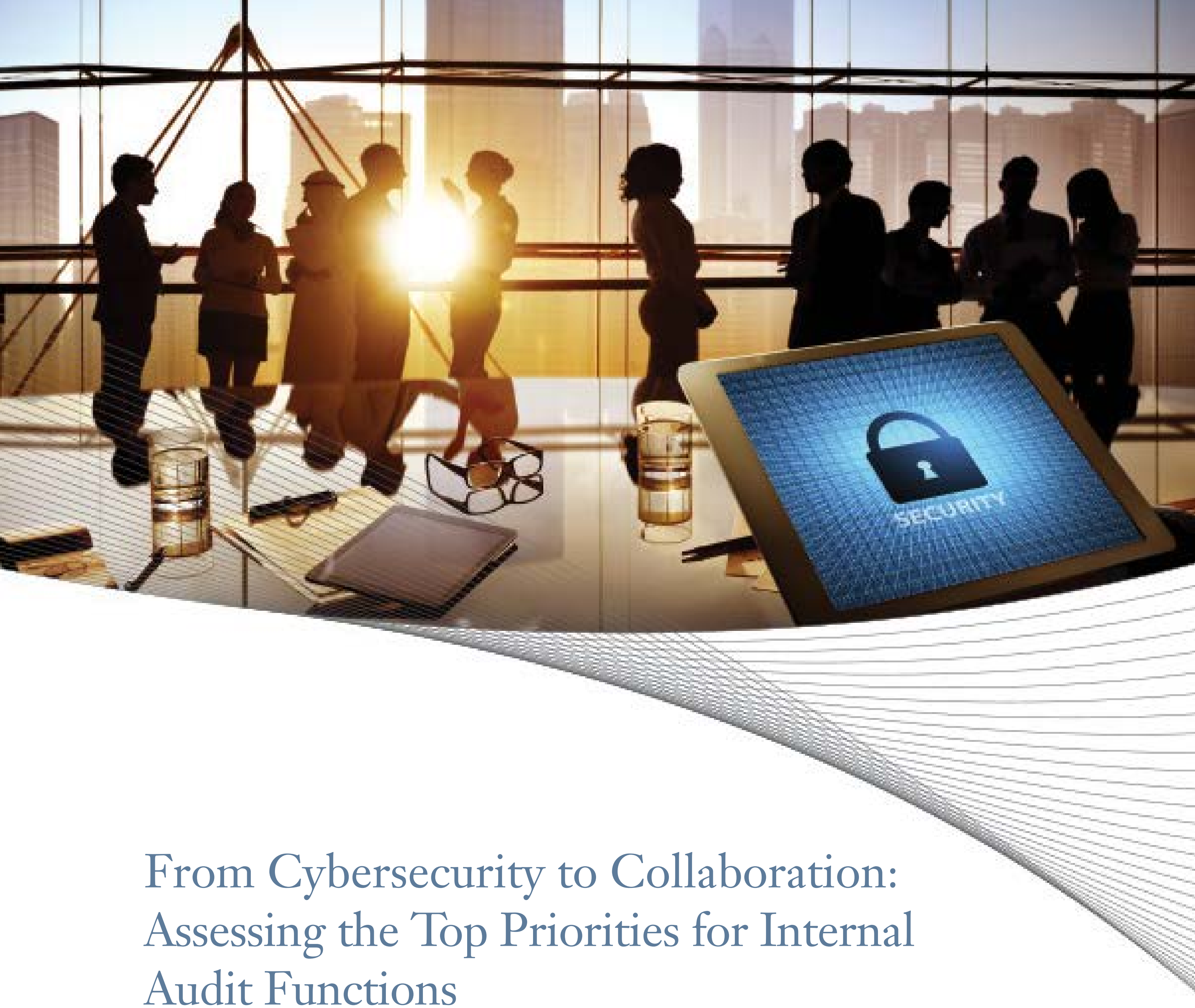


From Cybersecurity to Collaboration: Assessing the Top Priorities for Internal Audit Functions

2015 Internal Audit Capabilities and Needs Survey

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.®

> "SECURITY IS, I WOULD SAY, OUR TOP PRIORITY BECAUSE FOR ALL THE EXCITING THINGS YOU WILL BE ABLE TO DO WITH COMPUTERS – ORGANIZING YOUR LIVES, STAYING IN TOUCH WITH PEOPLE, BEING CREATIVE – IF WE DON'T SOLVE THESE SECURITY PROBLEMS, THEN PEOPLE WILL HOLD BACK."
>
> – Bill Gates[1]

Introduction

Will 2015 be a repeat of 2014 and become the year of the data breach? Organizations of all kinds and sizes are experiencing a troubling number of cybersecurity issues, challenges and breakdowns. IT departments clearly have major responsibilities in addressing these areas. But internal auditors also play a vital role in securing the organization by working closely with executive management and functional leaders to ensure that cybersecurity is incorporated into the flow of common business and its multitude of processes.

In this year's Internal Audit Capabilities and Needs Survey, we've devoted a special section to the current state of cybersecurity. Our findings show that, not surprisingly, cybersecurity represents a major focus for internal audit programs, but it is far from the only pressing issue on internal audit's plate.

- **Board engagement and the audit plan represent keys to effective cybersecurity –** When it comes to cybersecurity, top-performing organizations have both high board engagement as well as defined cybersecurity measures in the annual audit plan.
- **The list of internal audit priorities continues to grow –** There are cybersecurity issues; risks related to emerging technologies (e.g., social media, cloud computing and mobile applications); increasing regulatory compliance requirements; and new guidance and standards from The IIA, ISO and COSO. These and other priorities are requiring internal auditors to be nimble and adaptive in helping their organizations address rapidly evolving demands.
- **Technology-enabled auditing is on the rise –** Competing urgencies on a lengthy priorities list are driving more internal audit functions to increase their investment in, and use of, technology-enabled auditing approaches and tools.
- **More are focused on marketing and collaboration –** Internal audit leaders and staff are focused more than ever on conveying to the rest of the organization the function's mission, value and risk-related concerns. They also want to increase their collaboration as strategic partners with executive management, other functional leaders and the board to help the organization understand its risks and achieve its strategic objectives.

We sincerely appreciate the more than 800 chief audit executives and internal audit professionals who participated in our study this year. They represent a broad range of industries and organizations (see the Methodology and Demographics section for details). We are grateful for the time they invested in our study.

Finally, we once again acknowledge the tremendous global leadership provided by The Institute of Internal Auditors (IIA) in advancing the role of internal audit in business today.

[1] "One-on-One with Bill Gates," ABC News, February 16, 2005, www.abcnews.go.com/WNT/CEOProfiles/story?id=506354&page=1.

PASSWORD

Cybersecurity and the Audit Process

> "WE HAVE CORPORATE PRIVATE AS WELL AS PERSONAL PRIVATE INFORMATION THAT ARE AT RISK FROM AN EXTERNAL CYBERATTACK AS WELL AS FROM AN EMPLOYEE OR TRUSTED VENDOR THEFT."
>
> – Chief audit executive, midsize insurance company

Key Findings

- There is significant need for cybersecurity risk management improvement, with less than one in three organizations judging themselves to be "very effective" at managing cybersecurity risk to an acceptable level.
- "Top performers" are organizations that address cybersecurity risk in their audit plan and those whose board of directors is highly engaged with cybersecurity risk.
- Security of company information, brand and reputation damage, regulatory compliance, and loss of employees' personal information represent the greatest cybersecurity risks.

The magnitude and frequency of cybersecurity incidents continue to increase dramatically – in fact, those cyberattacks that are reported may only be "the tip of a vast iceberg."[2] A key question for CAEs and internal audit professionals to consider: What are the function's roles and responsibilities with regard to cybersecurity?

The growing importance of cybersecurity risks is evident not only in the findings in our special section, but also throughout this year's survey results. Internal audit leaders and professionals view strengthening data security, adhering to the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, and mastering new data analysis and auditing technology to be among their highest priorities. We receive similar feedback from our continuing interactions with CAEs and internal audit leaders, who, not surprisingly, have expressed a surge of interest in cybersecurity and data privacy issues. Other recent research from Protiviti[3] as well as the National Association of Corporate Directors[4] underscores cybersecurity's status as a major risk on the agenda for boards, executive management and internal audit to address.

Here, we assess the current state of cybersecurity risk in organizations, identify key enabling components of an effective cybersecurity risk management capability, and bring to light some of the differentiators that distinguish, in terms of cybersecurity, the leaders from the pack. We conclude by recommending 10 action items that CAEs and internal audit professionals should consider in their ongoing efforts to strengthen cybersecurity.

[2] *Board Perspectives: Risk Oversight*, Issue 44, "Managing Cybersecurity Risk," Protiviti, www.protiviti.com/en-US/Pages/Board-Perspectives-Risk-Oversight-Issue-44.aspx.

[3] See ISACA and Protiviti's *A Global Look at IT Audit Best Practices*, www.protiviti.com/ITAuditSurvey; and see Protiviti's *Bridging the Data Security Chasm: Assessing the Results of Protiviti's 2014 IT Security and Privacy Survey*, www.protiviti.com/ITSecuritySurvey.

[4] *Cybersecurity: A Boardroom Concern*, National Association of Corporate Directors, 2014, www.nacdonline.org.

Cybersecurity Top Performers – High Board Engagement, Audit Plan Focus

Through our analysis of the results, we have identified two critical success factors in establishing and maintaining effective cybersecurity measures:

1. **High level of engagement by the board of directors in cybersecurity**
2. **Evaluating cybersecurity risk as part of the current audit plan**

These results are detailed below and serve as key reference points in the discussion and analysis of our other survey results pertaining to cybersecurity.

How engaged is your board of directors with information security risks relating to your business?

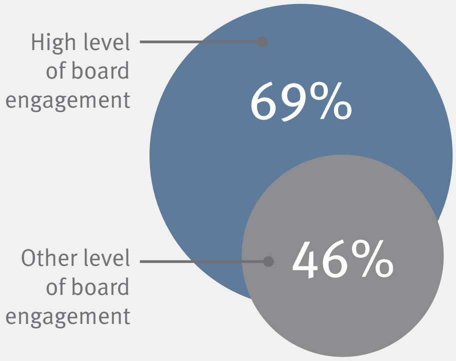
High engagement and level of understanding by the board	30%
Medium engagement and level of understanding by the board	41%
Low engagement and level of understanding by the board	14%
Don't know	15%

Is evaluating and auditing cybersecurity risk part of your audit plan?

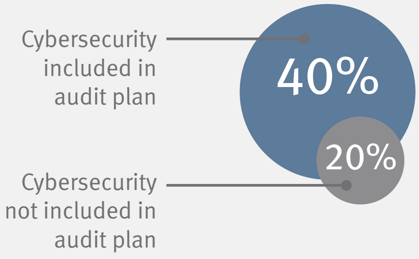
Yes, it is included in our current year audit plan	53%
No, but it will be included in next year's audit plan	27%
We have no plans to include it in the audit plan	20%

KEY FACTS

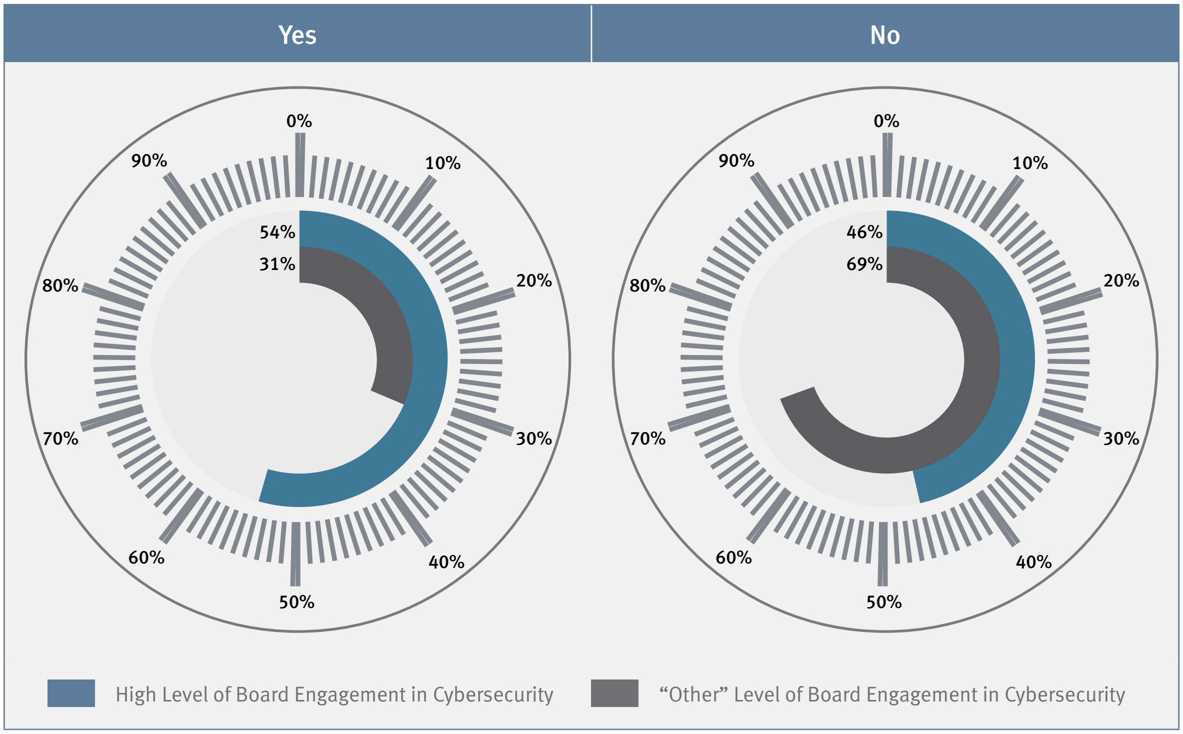
Percentage of organizations, by level of board engagement in information security risks, that include cybersecurity in the audit plan:



Percentage of organizations, by inclusion of cybersecurity in the current audit plan, whose board of directors has a high level of engagement in information security risks:



If cybersecurity is included in the audit plan, has internal audit evaluated the organization's cybersecurity program against the NIST Cybersecurity Framework?



Current State of Cybersecurity – An Internal Audit Perspective

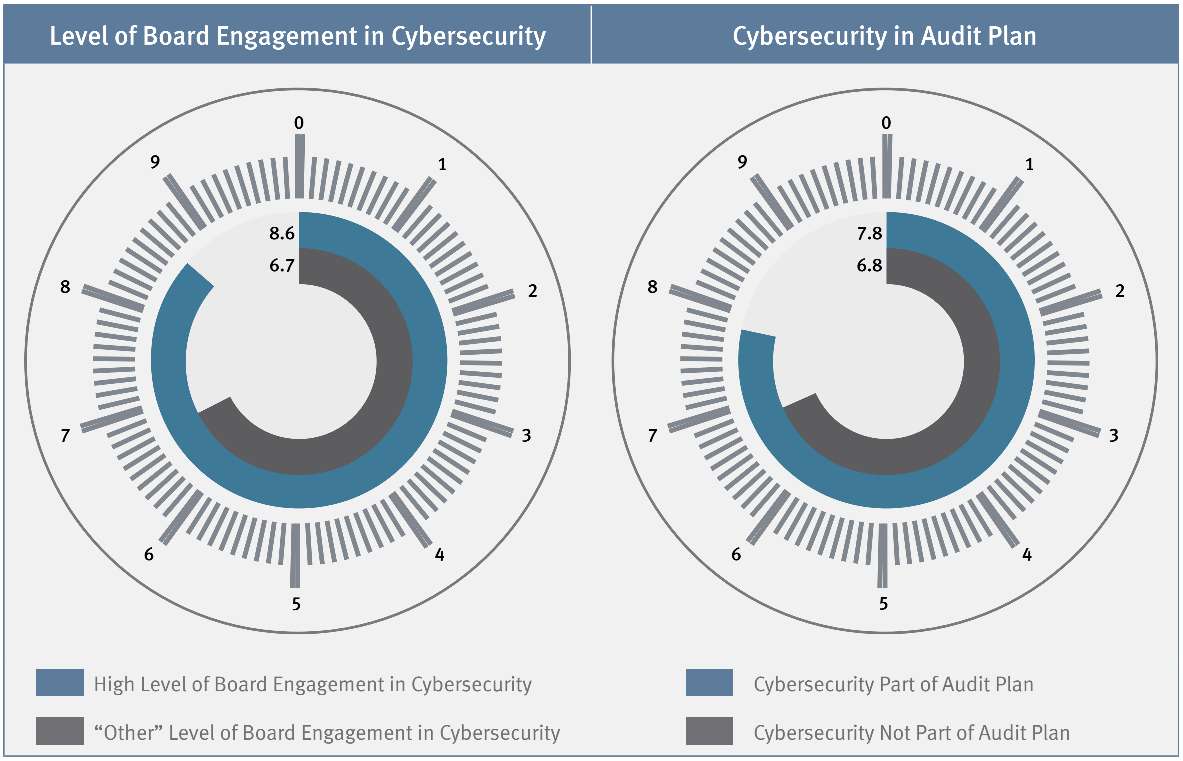
There is a clear need among most organizations to strengthen their ability to identify, assess and mitigate cybersecurity risk to an acceptable level, though "top performers" rate better in this regard.

Organizations that rate themselves "very effective" at identifying/assessing/mitigating cybersecurity risk to an acceptable level.

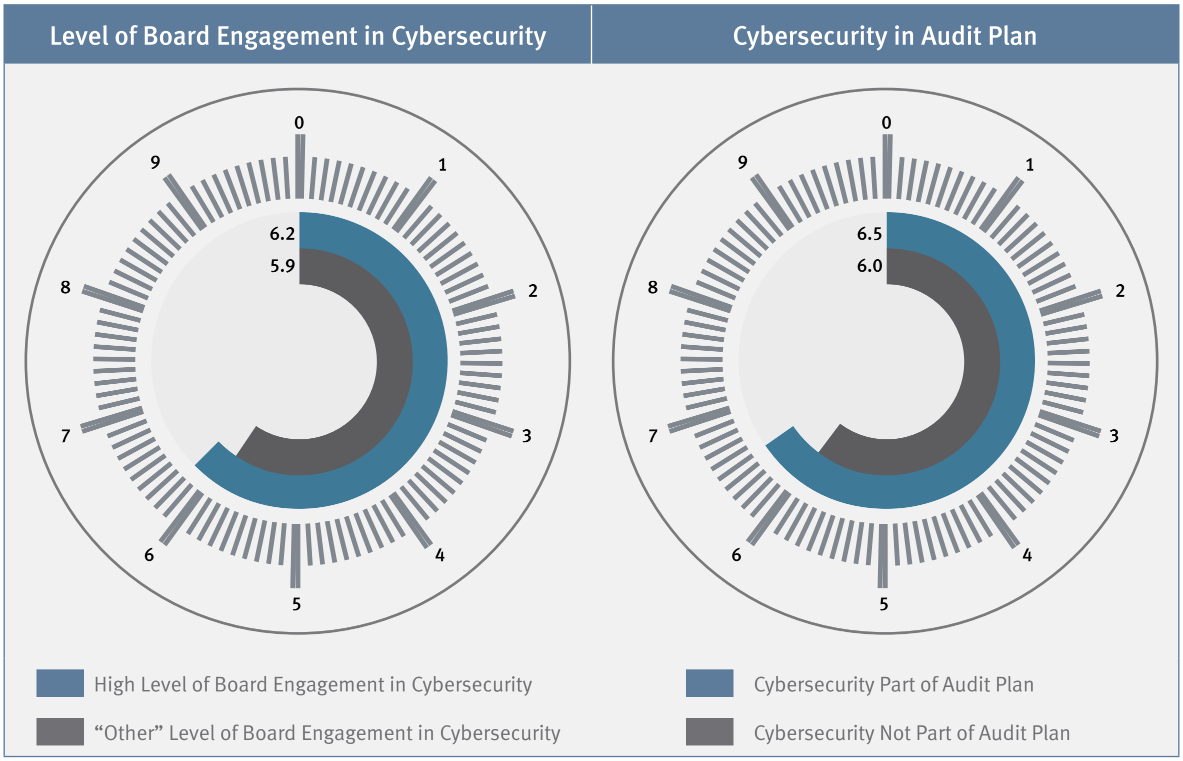
	High Level of Board Engagement	"Other" Level of Board Engagement	Cybersecurity Part of Audit Plan	Cybersecurity Not Part of Audit Plan
Identifying	47%	19%	35%	20%
Assessing	43%	19%	31%	21%
Mitigating	39%	15%	26%	18%

There is relatively strong awareness among management of the organization's information security exposure, particularly among "top performers." However, all respondents have less confidence in their organization's ability to prevent a cybersecurity breach by an employee or business partner (see charts on page 4).

On a scale of 1 to 10, where "10" is a high level of awareness and "1" is little or no awareness, rate senior management's level of awareness with regard to your organization's information security exposures.



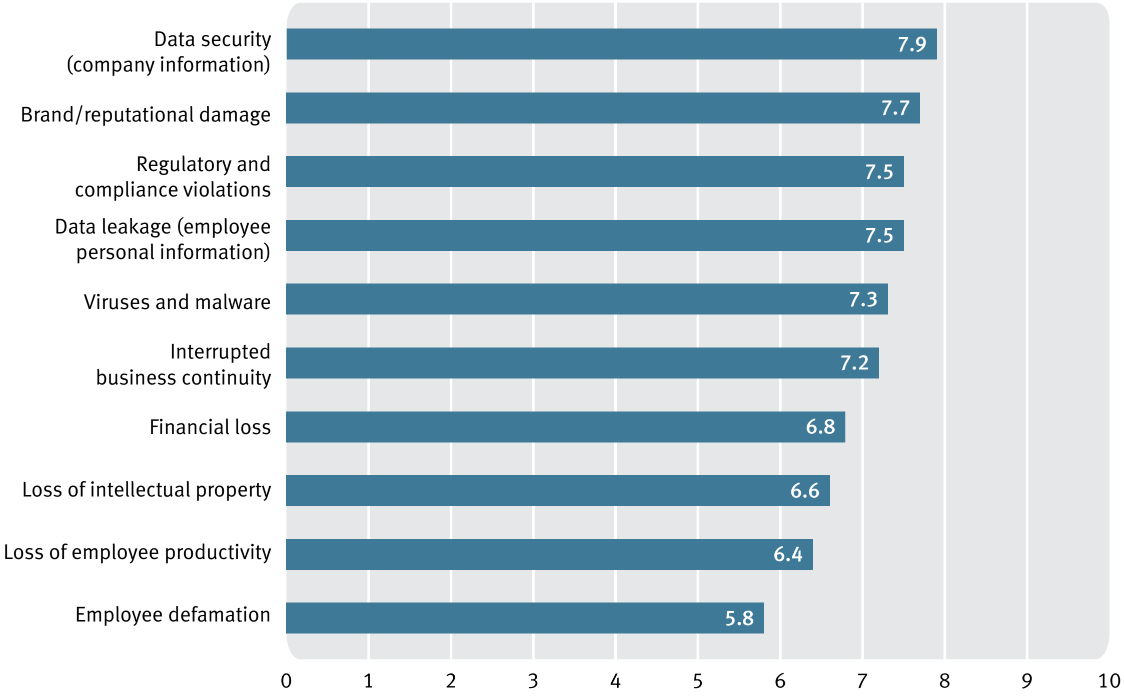
On a scale of 1 to 10, where "10" is a high level of confidence and "1" is little or no confidence, rate your level of confidence that your organization is able to prevent an opportunistic breach as a result of actions by a company insider (employee or business partner).



Security of company information, potential damage to the company's reputation and brand, regulatory compliance, and data leakage are viewed to be the most significant cybersecurity risks. In terms of the value of addressing cybersecurity risks, organizations view their ability to identify issues, risk or control problems early to be most important.

For each of the following areas, rate the level of cybersecurity risk it poses to your organization (with "10" posing the highest level of risk and "1" posing the lowest level of risk).

Base: All respondents



Where do you currently perceive the greatest value for addressing cybersecurity risk to your organization?

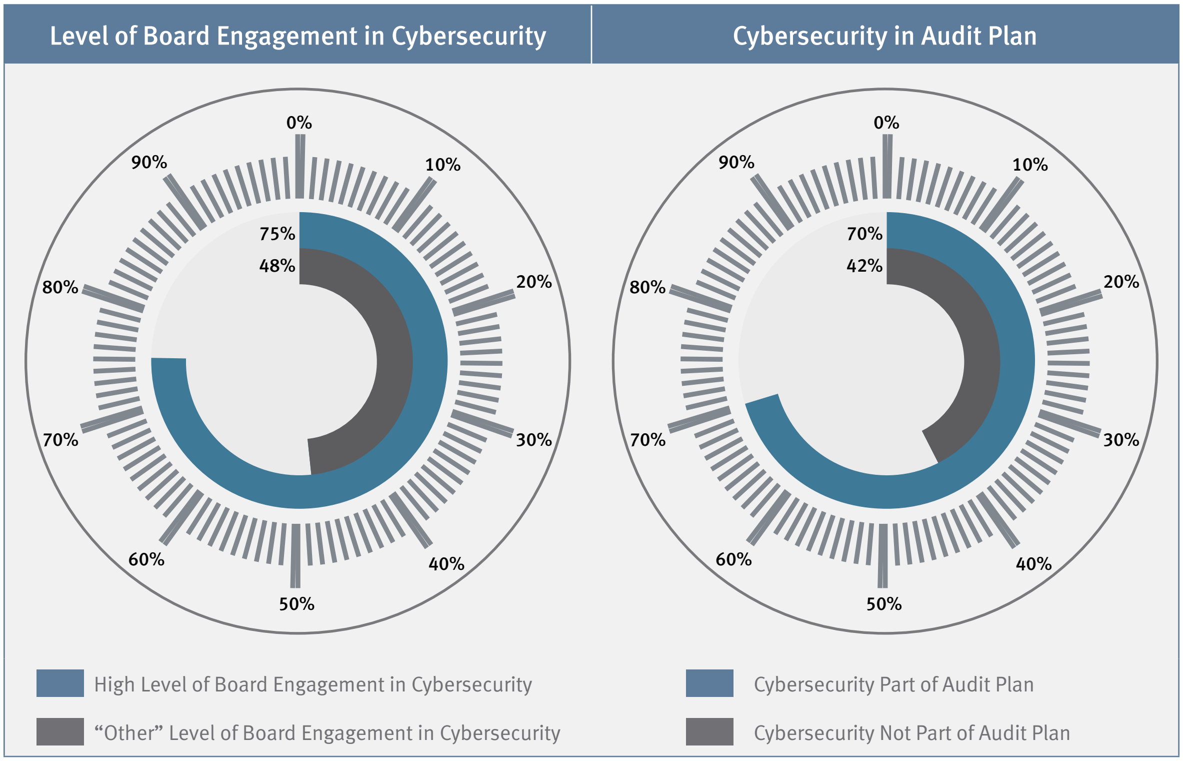
Base: All respondents

Earlier identification of issues, risk or control problems	40%
Regulatory compliance	16%
Monitor reputation risk	15%
Overall business strategy	11%
Validation of control effectiveness or failure	10%
Improved operational performance	5%
Cost recovery/improvement	3%

Assessing Cybersecurity Best Practices

Overall, more than half of organizations have a cybersecurity risk strategy and policy in place, with a clear gap between "top performers" and other organizations.

Does your organization have a cybersecurity risk strategy in place?*



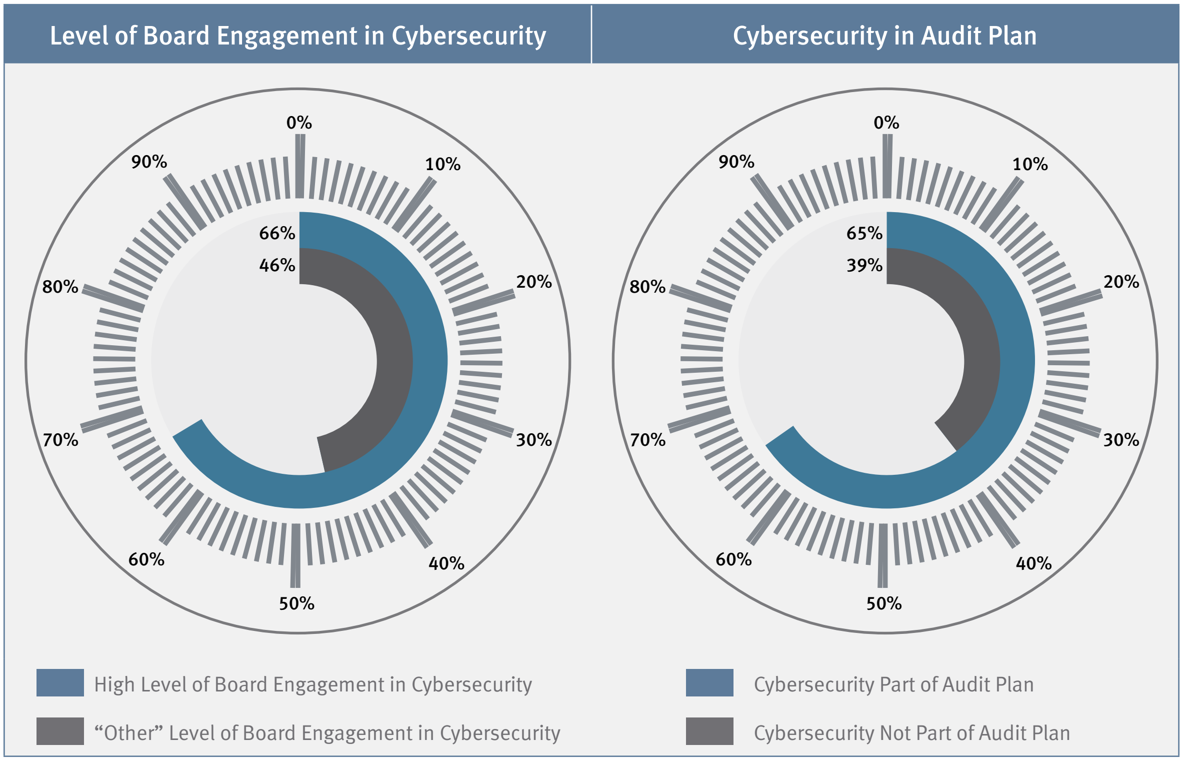
Level of Board Engagement in Cybersecurity

Cybersecurity in Audit Plan

** Shown: Percentages of "Yes" responses*

> "OUR ORGANIZATION HANDLES HIPAA PROTECTED DATA, SO THE RISK OF A BREACH IS SIGNIFICANT, AS PROTECTED HEALTHCARE DATA AND PERSONALLY IDENTIFIABLE INFORMATION COULD BE BREACHED."
>
> – Chief audit executive, midsize technology company

Does your organization have a cybersecurity policy in place?*



** Shown: Percentages of "Yes" responses*

It is encouraging to see that most organizations address cybersecurity risk via some form of risk assessment. Among those organizations that do so, the IT organization, external auditors, the audit committee and executive management have the most significant involvement (see tables on page 8).

Does your organization address cybersecurity risk in its risk assessment?

	High Level of Board Engagement	"Other" Level of Board Engagement	Cybersecurity Part of Audit Plan	Cybersecurity Not Part of Audit Plan
Yes, it is addressed separately from the overall risk assessment process	32%	22%	32%	17%
Yes, it is addressed as part of the overall risk assessment process	63%	56%	65%	49%
No	5%	22%	3%	34%

IF "YES": Please indicate the level of involvement of each of the following individuals/groups in assessing your organization's cybersecurity risk exposure.

	Significant	Moderate	Minimal	None
Audit committee	17%	43%	28%	12%
Company IT organization representatives	33%	47%	17%	3%
Executive management	44%	41%	13%	2%
External audit	20%	46%	28%	6%
Human resources	69%	27%	3%	1%
Internal audit/IT audit	48%	38%	11%	3%
Legal	31%	34%	19%	16%
Line of business executives	4%	27%	44%	25%
Management and/or process owners	13%	38%	34%	15%
Marketing/PR/corporate communications	4%	23%	43%	30%
Risk management (separate from internal audit)	18%	38%	32%	12%
Third-party service provider	13%	35%	28%	24%

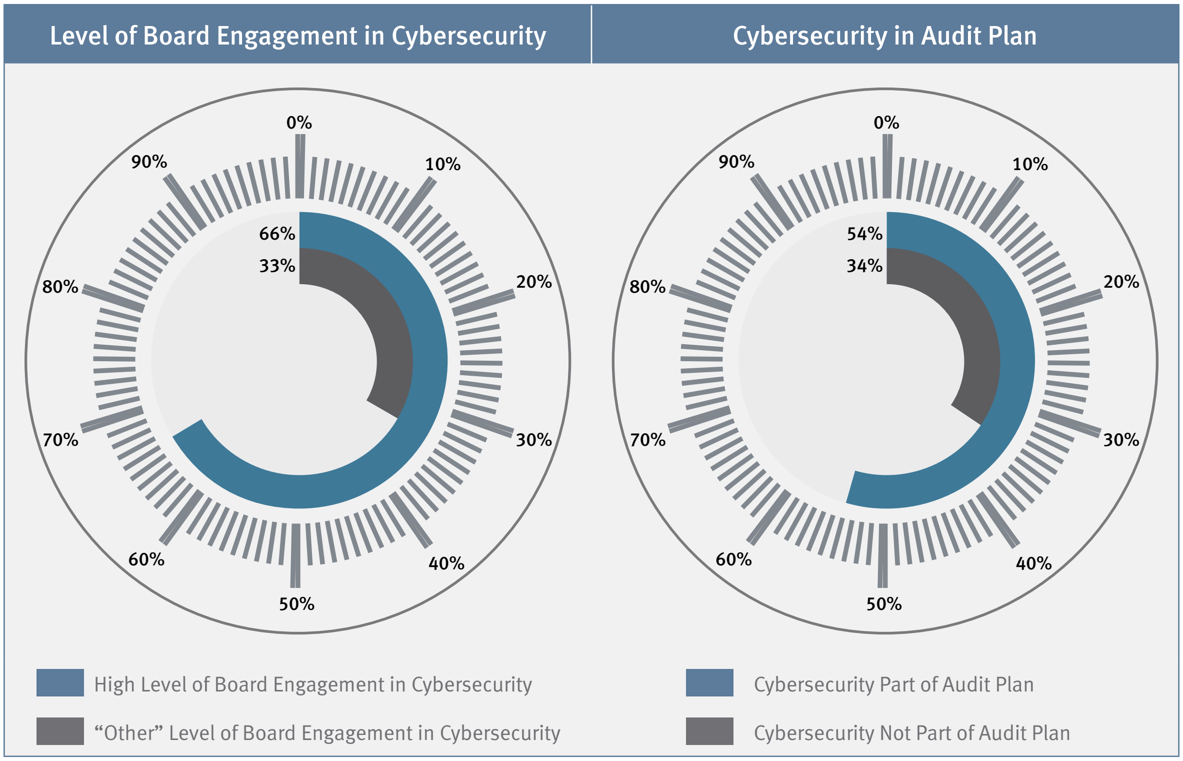
IF "YES": Please indicate the level of involvement of each of the following individuals/groups in assessing your organization's cybersecurity risk exposure.*

	High Level of Board Engagement	"Other" Level of Board Engagement	Cybersecurity Part of Audit Plan	Cybersecurity Not Part of Audit Plan
Audit committee	81%	48%	66%	51%
Company IT organization representatives	94%	73%	82%	78%
Executive management	91%	81%	86%	83%
External audit	81%	58%	67%	63%
Human resources	97%	96%	97%	94%
Internal audit/IT audit	93%	82%	94%	73%
Legal	85%	55%	70%	57%
Line of business executives	45%	23%	33%	26%
Management and/or process owners	64%	44%	55%	44%
Marketing/PR/corporate communications	45%	18%	28%	24%
Risk management (separate from internal audit)	73%	46%	59%	51%
Third-party service provider	59%	42%	55%	37%

* *Shown: Combined percentages of "Significant" and "Moderate" responses*

It also is positive to see that in many organizations, the CIO regularly reports to the audit committee on cybersecurity and IT risks, in general. Again, the numbers are significantly higher for "top performers."

Does the chief information officer (or equivalent position) regularly attend audit committee meetings to report on IT risks in general and specifically around cybersecurity?*



** Shown: Percentages of "Yes" responses*

KEY FACTS

30% Percentage of organizations that are not able to address specific areas of cybersecurity risk sufficiently in the audit plan due to lack of resources/skills.

22% Percentage of organizations that are not able to address specific areas of cybersecurity risk sufficiently due to lack of software tools.

Ten Cybersecurity Action Items for CAEs and Internal Audit

1. Work with management and the board to develop a cybersecurity strategy and policy.
2. Seek to have the organization become “very effective” in its ability to identify, assess and mitigate cybersecurity risk to an acceptable level.
3. Recognize the threat of a cybersecurity breach resulting from the actions of an employee or business partner.
4. Leverage board relationships to a) heighten the board’s awareness and knowledge of cybersecurity risk; and b) ensure that the board remains highly engaged with cybersecurity matters and up to date on the changing nature and strategic importance of cybersecurity risk.
5. Ensure cybersecurity risk is formally integrated into the audit plan.
6. Develop, and keep current, an understanding of how emerging technologies and technological trends are affecting the company and its cybersecurity risk profile.
7. Evaluate the organization’s cybersecurity program against the NIST Cybersecurity Framework, while recognizing that the framework does not go to the control level and therefore may require additional evaluations of ISO 27001 and 27002.
8. Recognize that with regard to cybersecurity, the strongest preventative capability requires a combination of human and technology security – a complementary blend of education, awareness, vigilance and technology tools.
9. Make cybersecurity monitoring and cyber-incident response a top management priority – a clear escalation protocol can help make the case for (and sustain) this priority.
10. Address any IT/audit staffing and resource shortages, which represents a top technology challenge in many organizations and can hamper efforts to address cybersecurity issues.

General Technical Knowledge

Key Findings

- IT-related risks and cybersecurity issues dominate a lengthy list of priorities for internal auditors.
- Strengthening data analysis capabilities according to The IIA's GTAG 16 (Data Analysis Technologies) marks a top priority for internal audit functions.
- Internal auditors increasingly consider and address cybersecurity and many other IT-related issues as *strategic* risks that require increased internal audit coverage.
- The NIST Cybersecurity Framework, which was finalized in 2014, remains a priority for internal audit, particularly as more cybersecurity legislative proposals are considered by Congress following the recent spate of high-profile cybersecurity incidents.[5]
- Mobile applications, cloud computing and social media applications represent top priorities, as these and related technological advancements create new risks.
- New – and newly important – guidance and standards from The IIA and ISO, as well as the 2013 COSO Internal Control Framework, remain top of mind; however, internal audit faces significant time and resource challenges integrating this guidance and these standards amid a rapidly growing set of IT-related priorities.

Overall Results, General Technical Knowledge

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	GTAG 16 – Data Analysis Technologies	2.5
2	NIST Cybersecurity Framework	2.2
3	Mobile applications	2.5
4	Practice Advisory 2320-4 – Continuous Assurance	2.8
5	The Guide to the Assessment of IT Risk (GAIT)	2.5

[5] www.whitehouse.gov/blog/2015/01/14/what-you-need-know-about-president-obama-s-new-steps-cybersecurity.

Commentary – Overall Findings

Respondents were asked to assess, on a scale of one to five, their competency in 35 areas of technical knowledge important to internal audit, with one being the lowest level of competency and five being the highest. For each area, they were then asked to indicate whether they believe their level of knowledge is adequate or requires improvement, taking into account the circumstances of their organization and industry. (For the areas of knowledge under consideration, see pages 13-14.) Figure 1 depicts a comparison of "Need to Improve" versus "Competency" ratings in a General Technical Knowledge landscape.

It is noteworthy that 12 of the top 13 priorities identified this year relate to IT risks, challenges and directives, including cybersecurity. What's more, the sole priority not directly related to IT – Practice Advisory 2120-3: Internal Audit Coverage of Risks to Achieving Strategic Objectives – will in many cases help auditors strengthen their IT risk management activities because more IT risks threaten the achievement of strategic objectives.

This isn't to say that IT risks represent the only priorities. Revised deadlines tied to aspects of the 2013 COSO Internal Control Framework loom. Feedback we've received from companies and internal audit leaders suggests COSO implementation has consumed significant internal audit time and effort. The need to address COSO, ISO and IIA-related priorities and evaluate and monitor numerous IT and data risks – given how social media applications, cloud computing and mobile technology continue to transform organizational risk – are pushing internal audit resources to their limits.

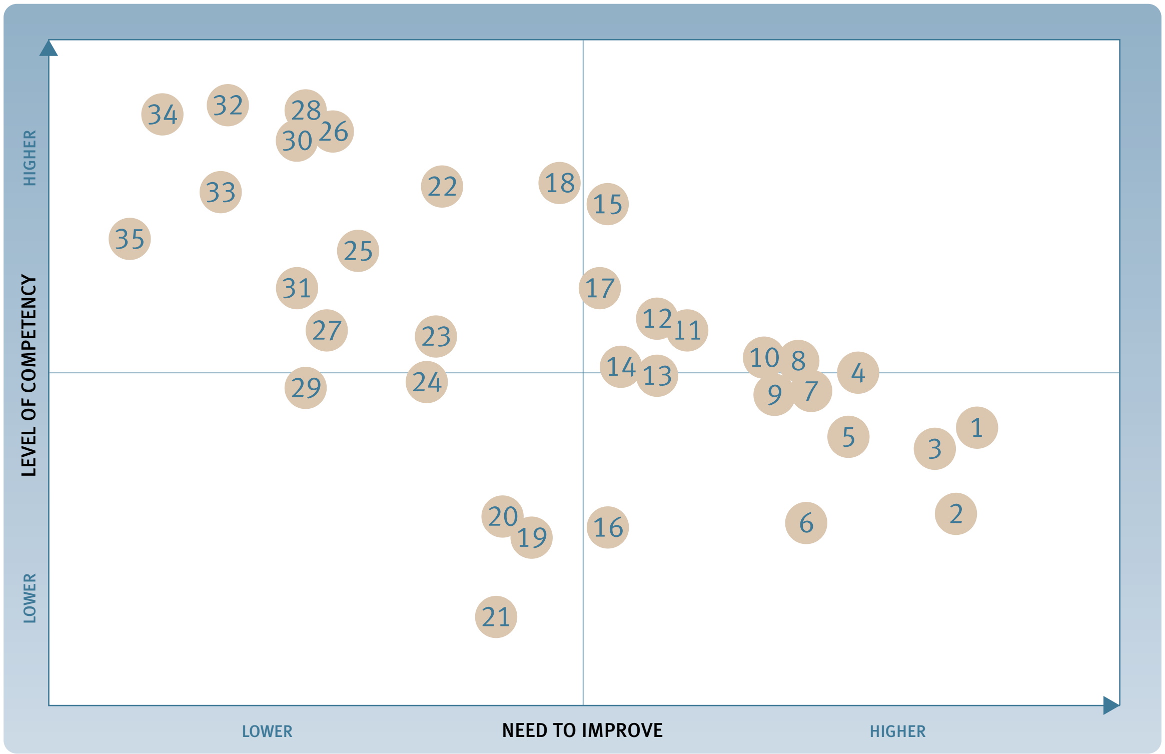
How internal audit meets these challenges will be determined by a number of factors, including their:

- Efficiency in addressing directives such as the NIST Cybersecurity Framework
- Ability to partner and collaborate effectively throughout the organization
- Access to outside expertise and best practices
- Ability to deploy technology to increase efficiency where possible and free up resources to focus more on strategic and complicated priorities

Internal Audit Action Items

- Given the strategic impact, highly volatile nature and likely long-term duration of cybersecurity and other IT risks, work with management to evaluate, monitor and strengthen the organization's ability to understand, identify and manage these risks.
- From a CAE perspective, ensure that IT and cybersecurity risks are understood and monitored as a strategic-level risk, when warranted, and as a matter for the board of directors to monitor regularly.
- As more functions and groups within the organization increase their use of data, social media, cloud computing and mobile technology, work in a collaborative manner throughout the enterprise to develop and continually update strategies and policies for managing these business tools in a risk-savvy manner.
- Remain vigilant to ensure fraud detection and fraud prevention activities are keeping pace as the organization's fraud risk profile changes due to the introduction of new data analysis, social media, mobile and cloud computing applications.

Figure 1: General Technical Knowledge – Perceptual Map



Number	General Technical Knowledge	Number	General Technical Knowledge
1	GTAG 16 – Data Analysis Technologies	12	IT governance
2	NIST Cybersecurity Framework	13	COBIT
3	Mobile applications	14	Practice Guide – Auditing Anti-bribery and Anti-corruption Programs
4	Practice Advisory 2320-4 – Continuous Assurance	15	2013 COSO Internal Control Framework – Evaluation of “Presence, Functioning and Operating Together”
5	The Guide to the Assessment of IT Risk (GAIT)	16	ISO 31000 (risk management)
6	ISO 27000 (information security)	17	IIA International Professional Practices Framework (IPPF) Exposure Draft (proposed in 2014)
7	Cloud computing	18	Fraud risk management
8	GTAG 17 – Auditing IT Governance	19	ISO 9000 (quality management and quality assurance)
9	Social media applications	20	Six Sigma
10	Practice Advisory 2120-3 – Internal Audit Coverage of Risks to Achieving Strategic Objectives	21	ISO 14000 (environmental management)
11	Practice Guide – Business Continuity Management	22	COSO Enterprise Risk Management Framework

Number	General Technical Knowledge	Number	General Technical Knowledge
23	Revenue Recognition Standard (Financial Accounting Standards Board Accounting Standards Update No. 2014-09)	30	2013 COSO Internal Control Framework – Information and Communication
24	Country-specific enterprise risk management framework	31	Overall Opinions (Standard 2450)
25	Reporting on Controls at a Service Organization – SSAE 16 / AU 324 (replaces SAS 70)	32	2013 COSO Internal Control Framework – Control Activities
26	2013 COSO Internal Control Framework – Monitoring Activities	33	Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)
27	Functional Reporting Interpretation (Standard 1110)	34	2013 COSO Internal Control Framework – Control Environment
28	2013 COSO Internal Control Framework – Risk Assessment	35	Corporate social responsibility
29	International Financial Reporting Standards (IFRS)		

Overall Results, General Technical Knowledge – Three-Year Comparison

2015	2014	2013
GTAG 16 – Data Analysis Technologies	Mobile applications	Social media applications
NIST Cybersecurity Framework	NIST Cybersecurity Framework	Recently enacted IIA Standard – Functional Reporting Interpretation (Standard 1110)
Mobile applications		Recently enacted IIA Standards – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)
Practice Advisory 2320-4: Continuous Assurance	Social media applications	GTAG 16 – Data Analysis Technologies
		Recently enacted IIA Standard – Overall Opinions (Standard 2450)
		Cloud computing
The Guide to the Assessment of IT Risk (GAIT)	Cloud computing	The Guide to the Assessment of IT Risk (GAIT)
		GTAG 13 – Fraud Prevention and Detection in an Automated World
		ISO 27000 (information security)
		COSO Internal Control Framework (DRAFT 2012 version)
	GTAG 16 – Data Analysis Technologies	Practice Guide – Assessing the Adequacy of Risk Management
		GTAG 6 – Managing and Auditing IT Vulnerabilities
		Fraud risk management

More on the NIST Cybersecurity Framework

When it comes to assessing the strength of current cybersecurity measures, the NIST Cybersecurity Framework can serve as a useful litmus test for organizations and internal audit functions. Many qualities of this framework also describe key aspects of leading practices within internal audit. It technically is voluntary in the regulatory sense (yet all but required from a governance perspective), it is risk-based, it is complementary with other risk programs, and it is subject to change and enhancement.

More internal audit functions are discovering that the NIST framework's approach mirrors their existing program assessments:

1. Define the business priorities and the scope of the [cybersecurity] program.
2. Define the assets in scope and the threats to them.
3. Create an "As Is" or baseline profile of the organization's security program implementation.
4. Perform a risk assessment of the organization's readiness.
5. Create a "To Be" statement/objective for the security program.
6. Define gaps between the "As Is" and "To Be" states, assess their impact and prioritize remediation activities.

With regard to the last point, these gaps are, of course, crucial. Internal auditors witness this type of gap when realizing that the NIST framework is incomplete, in that it does not reach the control level, where ISO 27000 (information security) standards can be applied. Savvy internal auditors are adept at filling a wide range of risk-management and knowledge gaps. That helps explain why ISO 27000 (information security) ranks among the top 10 priorities for internal auditors this year.

> "CYBERSECURITY IS SOMETHING THAT THE AUDIT TEAM TAKES VERY SERIOUSLY ... IT HANDLES IDENTIFYING THE RISKS AND ADDRESSING ANY POTENTIAL THREATS WITH THE BUSINESS."
>
> – Audit staff member, large insurance company

Focus on Results by Company Size

Company Size Results, General Technical Knowledge		
Small ‹ US$1B	Medium US$1B-$9B	Large › US$10B
GTAG 16 – Data Analysis Technologies	NIST Cybersecurity Framework	Mobile applications
The Guide to the Assessment of IT Risk (GAIT)	Mobile applications	GTAG 16 – Data Analysis Technologies
NIST Cybersecurity Framework	GTAG 16 – Data Analysis Technologies	NIST Cybersecurity Framework
Mobile applications	Practice Advisory 2120-3 – Internal Audit Coverage of Risks to Achieving Strategic Objectives	ISO 31000 (risk management)
GTAG 17 – Auditing IT Governance	Practice Advisory 2320-4 – Continuous Assurance	ISO 27000 (information security)

Focus on Chief Audit Executives

The responses from CAEs are generally consistent with the overall results. However, there are several subtle differences (e.g., the NIST Cybersecurity Framework sitting atop the CAE priority list) that suggest cybersecurity-related concerns and IT risks remain among the most critical areas for CAEs to address in the coming year.

CAE Results, General Technical Knowledge		
"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	NIST Cybersecurity Framework	2.2
2	Mobile applications	2.4
3	GTAG 16 – Data Analysis Technologies	2.7
4	The Guide to the Assessment of IT Risk (GAIT)	2.6
5	ISO 27000 (information security)	2.1

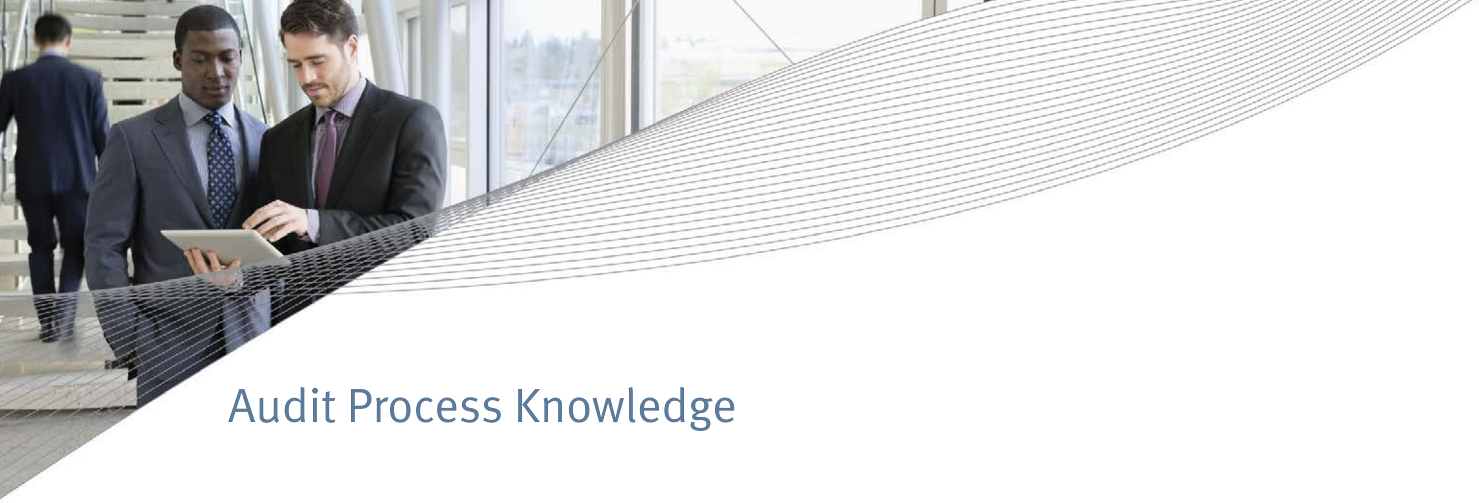
> "INFORMATION PRIVACY IS HIGHLY VALUED, SO ANY INTERNAL LEAK IS CONSIDERED SERIOUS, EVEN THOUGH THE TRUE IMPACT MAY BE MINIMAL."
>
> – Director of auditing, large manufacturing company

Key Questions for CAEs

- Are the CAE, CEO, CIO, CMO, chief human resources officer, and other C-suite and business-unit executives engaged and collaborating with each other (and with the board, when relevant) for the purpose of understanding new IT and cybersecurity risks and regulatory directives?
- How are you and your team determining if current risk management capabilities, processes, technology and talent are sufficient?
- Is your board engaged and informed of the quickly changing nature of IT and cybersecurity risks?
- Does the internal audit function have a mechanism for monitoring breaking IT/cybersecurity risks and regulatory responses?
- Does the internal audit function incorporate assessments of IT (and cybersecurity), including evaluations of social media and mobile application risk, in the audit plan?
- Are your current internal audit resources and expertise sufficient given the magnitude of IT risk and the speed with which it can change and strike?
- What mechanisms are you using to ensure that key regulatory requirements and related guidance are given sufficient attention and resources?

CAE Results, General Technical Knowledge – Three-Year Comparison

2015	2014	2013
NIST Cybersecurity Framework	Mobile applications	Social media applications
Mobile applications	Cloud computing	Recently enacted IIA Standard – Functional Reporting Interpretation (Standard 1110)
GTAG 16 – Data Analysis Technologies	NIST Cybersecurity Framework	COSO Internal Control Framework (DRAFT 2012 version)
The Guide to the Assessment of IT Risk (GAIT)	GTAG 16 – Data Analysis Technologies	
ISO 27000 (information security)	Social media applications	Recently enacted IIA Standards – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)
	GTAG 6 – Managing and Auditing IT Vulnerabilities	Cloud computing
		ISO 27000 (information security)



Audit Process Knowledge

Key Findings

- Internal auditors remain committed to leveraging technology-enabled auditing – including CAATs and data analysis tools – to achieve a more detailed, real-time picture of their organization's processes, controls and risks.
- Internal audit also remains focused on monitoring fraud, statistical analysis and continuous auditing.
- Marketing internal audit internally ranks among the top priorities for CAEs as well as all internal auditing professionals.

Overall Results, Audit Process Knowledge		
"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1 (tie)	Auditing IT – security	2.9
	Computer-assisted audit tools (CAATs)	3.1
3	Data analysis tools – data manipulation	3.2
4	Marketing internal audit internally	3.4
5	Fraud – monitoring	3.5

Commentary – Overall Findings

Respondents were asked to assess, on a scale of one to five, their competency in 36 areas of audit process knowledge, with one being the lowest level of competency and five being the highest. For each area, they were then asked to indicate whether they believe their level of knowledge is adequate or requires improvement, taking into account the circumstances of their organization and industry. (For the areas of knowledge under consideration, see page 21.) Figure 2 depicts a comparison of "Need to Improve" versus "Competency" ratings in an Audit Process Knowledge landscape.

Technology and marketing have become crucial success factors for internal auditors. Although, as detailed earlier in our report, emerging technologies pose sizeable organizational challenges, they also present significant opportunities, especially to internal audit functions that learn to leverage technology-enabled auditing.

Technology-enabled auditing equips auditors with a real-time, high-definition picture of organizational processes and controls. These snapshots also help shed light on opportunities to improve process effectiveness and efficiencies. Technology can help automate ongoing monitoring of certain internal controls, track issues, and provide customized dashboards and exception-reporting capability. The intelligent application of continuous auditing and CAATs techniques, combined with data mining and data analysis tools, expands internal audit's reach and the effectiveness of its risk coverage.

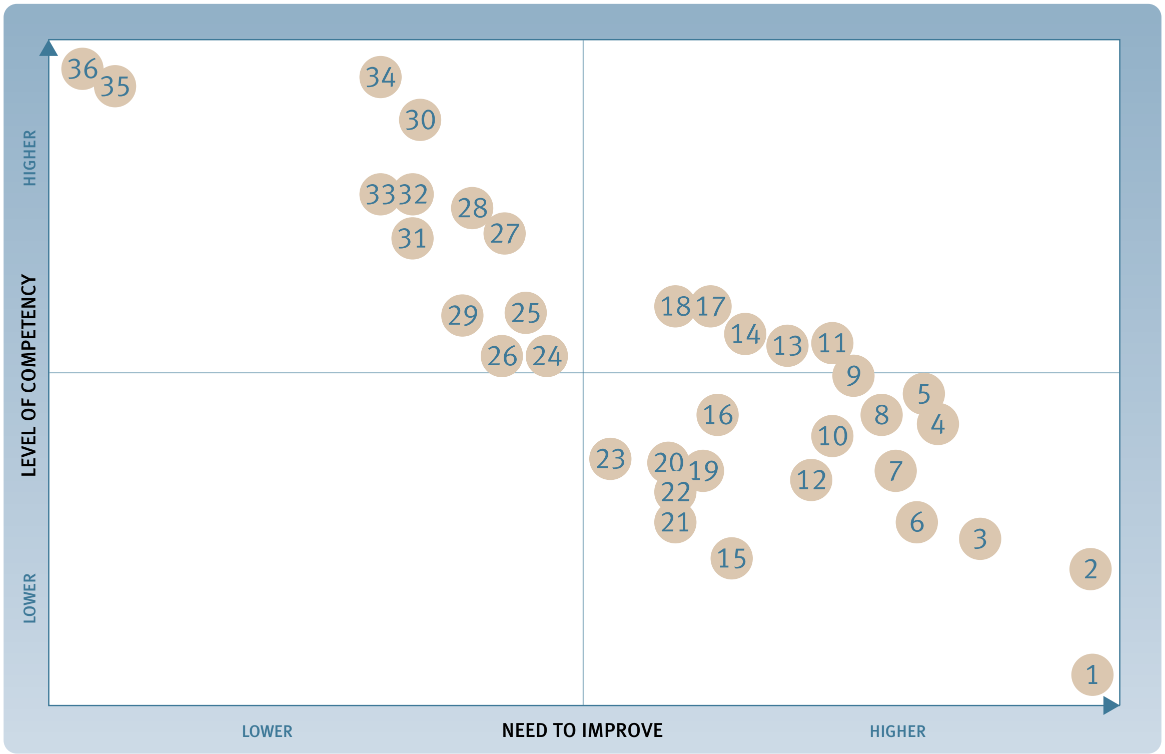
What is rather puzzling is how these findings remain so consistent in every year of our study. Not only do capabilities such as CAATs and data analysis tools annually land at or near the top of the list of internal audit areas in need of improvement, but the competency scores stay remarkably consistent. In fact, when we compared competency scores over the past five years for CAATs, data analysis tools (data manipulation), continuous auditing and continuous monitoring, we found that the scores for each did not vary over this period by more than three-tenths of a point (on our five-point scale).

What does this mean? There continues to be significant dialogue among internal audit functions about the need to leverage technology-enabled auditing tools, but they are not achieving progress. At this juncture, CAEs and internal audit leaders should consider whether this is becoming a never-ending journey. Will technology-enabled auditing become a reality in the organization, or will it continue to be discussed but not implemented? What needs to change so that these tools are not continually on the horizon for internal audit functions? Only by addressing these questions head-on can internal audit departments hope to achieve measurable and meaningful progress.

Internal Audit Action Items

- Leverage technology-enabled auditing by applying CAATs, continuous monitoring and data analysis tools to the greatest extent possible to achieve efficiencies in assessing risk, expanding audit coverage, automating critical internal controls, tracking issues, providing exception reports, and mining and analyzing data.
- Through technology-enabled auditing, draw meaningful insights regarding emerging risks and process and control performance.
- Assess the degree to which current expertise within the internal audit function enables it to harness the value of new IT systems, applications and tools; data analysis approaches; and technology- and data-related fraud detection and prevention.
- Market internal audit's capabilities and values through relationship-building at all levels of the organization (including the board) and through practical demonstrations of internal audit's expertise.
- Ensure that the highest levels of the organization – particularly the CEO, CFO and audit committee members – understand the value technology-enabled auditing can deliver, along with the potential for additional investments in these tools and related technologies that support continuous monitoring and auditing as well as advanced data analysis techniques.
- Remain vigilant with respect to fraud and how organizational changes affect the company's fraud risk profile.

Figure 2: Audit Process Knowledge – Perceptual Map



Applying these technologies also helps on personal and interpersonal levels. By using technology, internal audit can devote more time and effort to building relationships with process and functional owners and providing expertise in high-impact areas.

And this ties into another key priority for internal audit. Our results show that, from an internal marketing perspective, internal auditors want to raise awareness among the rest of the organization of their capabilities and value. Internal audit leaders continue to seek opportunities for more strategic-level responsibilities and closer collaboration with other departments.

This relationship-building serves as a highly effective form of internal marketing by demonstrating internal audit's value to the organization and educating business colleagues about internal audit's capabilities.

Number	Audit Process Knowledge	Number	Audit Process Knowledge
1	Auditing IT – security	19	Quality Assurance and Improvement Program (IIA Standard 1300) – Periodic Reviews (IIA Standard 1311)
2	Computer-assisted audit tools (CAATs)	20	Quality Assurance and Improvement Program (IIA Standard 1300) – Ongoing Reviews (IIA Standard 1311)
3	Data analysis tools – data manipulation	21	Auditing IT – computer operations
4	Marketing internal audit internally	22	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (Standard 1312)
5	Fraud – monitoring	23	Auditing IT – continuity
6	Data analysis tools – statistical analysis	24	Operational auditing – cost effectiveness/ cost reduction
7	Continuous auditing	25	Self-assessment techniques
8	Assessing risk – emerging issues	26	Auditing IT – change control
9	Fraud – fraud risk	27	Assessing risk – process, location, transaction level
10	Continuous monitoring	28	Assessing risk – entity level
11	Fraud – management/prevention	29	Operational auditing – effectiveness, efficiency and economy of operations approach
12	Auditing IT – new technologies	30	Presenting to senior management
13	Fraud – fraud risk assessment	31	Statistically based sampling
14	Fraud – fraud detection/investigation	32	Top-down, risk-based approach to assessing internal control over financial reporting
15	Auditing IT – program development	33	Operational auditing – risk-based approach
16	Data analysis tools – sampling	34	Report writing
17	Enterprisewide risk management	35	Audit planning – process, location, transaction level
18	Fraud – auditing	36	Audit planning – entity level

Overall Results, Audit Process Knowledge – Three-Year Comparison

2015	2014	2013
Auditing IT – security	CAATs	Data analysis tools – data manipulation
CAATs		Fraud – monitoring
Data analysis tools – data manipulation	Data analysis tools – data manipulation	Auditing IT – new technologies
Marketing internal audit internally		Fraud – fraud risk assessment
Fraud – monitoring	Data analysis tools – statistical analysis	Data analysis tools – statistical analysis
		Fraud – fraud detection/investigation
	Auditing IT – new technologies	Fraud – management/prevention
		CAATs
	Data analysis tools – sampling	Data analysis tools – sampling

Focus on Results by Company Size

Company Size Results, Audit Process Knowledge

Small ‹ US$1B	Medium US$1B-9B	Large › US$10B
Auditing IT – security	CAATs	Auditing IT – security
CAATs	Assessing risk – emerging issues	Auditing IT – program development
Data analysis tools – statistical analysis	Data analysis tools – data manipulation	Marketing internal audit internally
Fraud – monitoring	Auditing IT – security	Auditing IT – new technologies
Continuous auditing	Continuous auditing	CAATs
Marketing internal audit internally		Data analysis tools – data manipulation

Focus on Chief Audit Executives

Feedback from CAEs in the survey parallels the overall response. CAEs remain committed to marketing their functions internally and focusing on a wide range of technology-enabled auditing tools and techniques.

CAE Results, Audit Process Knowledge		
"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1 (tie)	Auditing IT – security	2.8
	Computer-assisted audit tools (CAATs)	3.1
3	Data analysis tools – data manipulation	3.1
4	Continuous auditing	3.3
5	Data analysis tools – statistical analysis	3.2

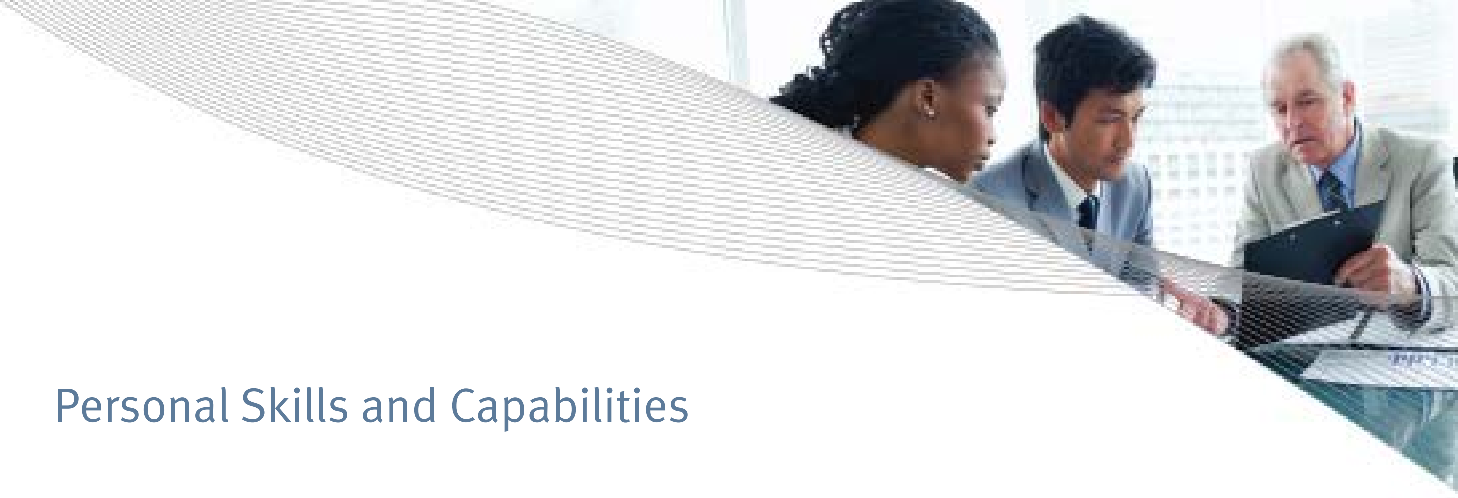
Key Questions for CAEs

- Is your internal audit team aware of a consistent message regarding your function's value and expertise? Are they communicating and demonstrating this value and expertise to the business through all of their work and relationship-building activities?
- Are the CEO, CFO, CIO, audit committee members and the rest of the board well-informed of the value that technology-enabled auditing offers from a risk management perspective?
- How is your function using technology-enabled auditing tools and techniques to carve out more time for strategic consultations with the business, assess new and emerging risks, and strengthen its collaborations throughout the organization?
- How do you ensure the level of training your internal auditors receive, especially training related to technology-enabled auditing tools, is sufficient?
- Do you maintain longer-term talent management plans with a focus on difficult-to-find types of internal auditing expertise (e.g., IT auditing)?

CAE Results, Audit Process Knowledge – Three-Year Comparison

2015	2014	2013
Auditing IT – security	Auditing IT – new technologies	Data analysis tools – data manipulation
CAATs	CAATs	
Data analysis tools – data manipulation	Data analysis tools – data manipulation	Auditing IT – new technologies
Continuous auditing	Marketing internal audit internally	
Data analysis tools – statistical analysis	Data analysis tools – statistical analysis	Data analysis tools – sampling
		CAATs
		Data analysis tools – statistical analysis
		Fraud – fraud risk assessment

> "THE LARGEST [CYBERSECURITY] RISK WE FACE IS TO THE BRAND AND CORPORATE IMAGE IN THE EVENT ANY PERSONALLY IDENTIFIABLE INFORMATION OR PROPRIETARY INFORMATION IS LOST OR STOLEN."
>
> – IT audit staff, large retail organization



Personal Skills and Capabilities

Key Findings

- Using/mastering new technology and applications is a clear priority for CAEs as well as all internal audit professionals.
- Persuasion, developing other board committee relationships, strategic thinking and time management also rank as top priorities.
- Internal auditors are committed to improving and leveraging their personal skills (e.g., persuasion), relationships (e.g., with all board committees, including the audit committee), and internal and external networks (e.g., leveraging others' expertise) to balance multiple priorities and strengthen the function's strategic contributions to the organization.

Overall Results, Personal Skills and Capabilities

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Using/mastering new technology and applications	3.6
2	Persuasion	3.6
3	Developing other board committee relationships	3.2
4	Strategic thinking	3.8
5	Time management	3.7

Commentary – Overall Findings

Respondents were asked to assess, on a scale of one to five, their competency in 19 areas of personal skills and capabilities, with one being the lowest level of competency and five being the highest. For each area, respondents were then asked to indicate whether they believe their level of knowledge is adequate or requires improvement, taking into account the circumstances of their organization and industry. (For the areas of knowledge under consideration, see page 27.) Figure 3 depicts a comparison of "Need to Improve" versus "Competency" ratings in a Personal Skills and Capabilities landscape.

Given an overflowing priority list and the rapidly changing nature of organizational risks, internal auditors are tasked with executing a difficult, delicate balancing act. Not surprisingly, they are turning to technology to help them achieve this balance. It is understandable that using/mastering new technology and applications figures as the highest priority, in terms of personal skills, for internal auditors and CAEs.

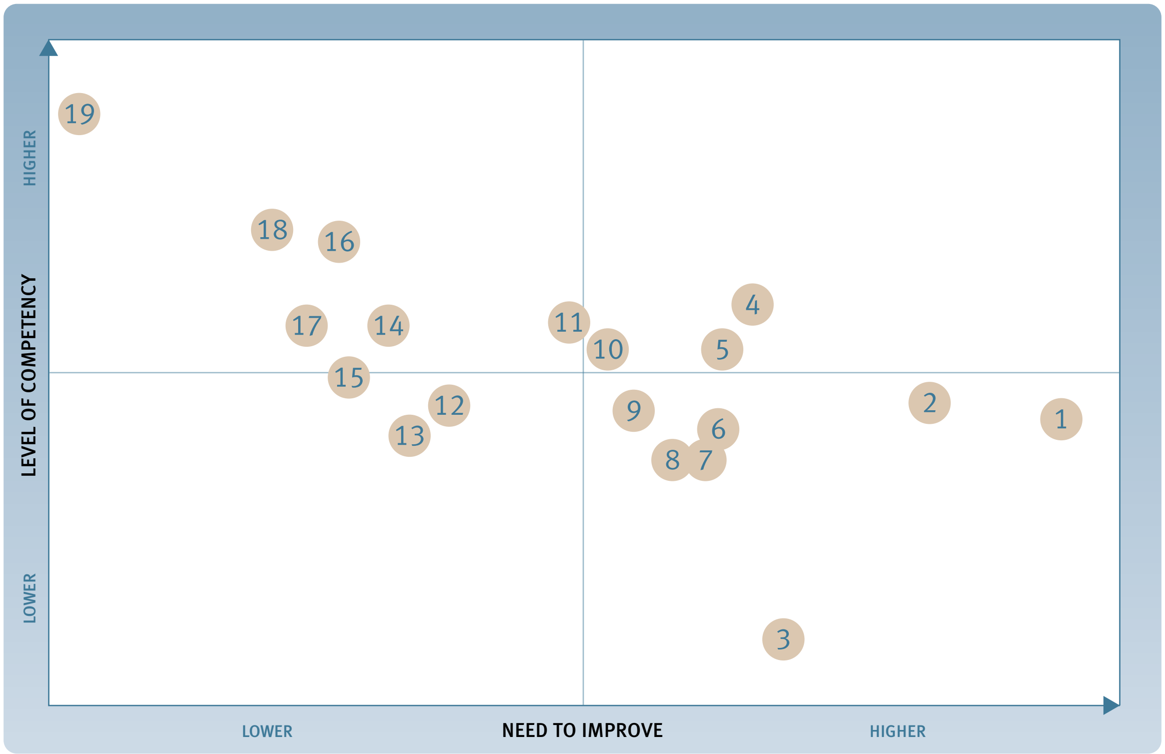
As noted earlier, although technology (in the guise of cyberthreats, for example) poses sizeable risks, it also presents valuable opportunities. Technology-enabled auditing delivers substantial benefits with regard to efficiency and effectiveness. And on a personal level, technology performs double-duty as an increasingly valuable internal audit skill. By mastering continuous auditing, data analysis and other technology tools, internal auditors fortify the value of their personal brands while freeing them to invest more time in strategic endeavors when time is a precious asset.

Balancing internal audit's multiple priorities – regulatory compliance and financial reporting controls compliance; risk-based activities linked to the organization's strategies and objectives; core assurance activities rotated over several audit periods; and investigations, special projects and other management requests – requires sharp interpersonal skills. Chief among these abilities are strategic thinking, persuasion, time management, presenting and related skills that serve to strengthen the collaborative partnerships that internal auditors make throughout the organization, with the board and with external experts.

Internal Audit Action Items

- Ensure internal auditors have access to experiences and training that help them use and master new technology and applications.
- Seek out other opportunities (e.g., stretch assignments, job rotations and work alongside outside experts) to help internal audit staff develop and strengthen their skills in communication and collaboration.
- Recognize the increasing importance of time-management skills given the bulging workloads and competing priorities confronting most internal audit functions.
- Seek to expand informal professional networks inside and outside the organization as a way to gain exposure to different kinds of expertise that help the internal auditor operate more strategically, more collaboratively and under greater pressure.

Figure 3: Personal Skills and Capabilities – Perceptual Map



Number	Personal Skills and Capabilities	Number	Personal Skills and Capabilities
1	Using/mastering new technology and applications	11	Dealing with confrontation
2	Persuasion	12	Leadership (within your organization)
3	Developing other board committee relationships	13	Developing audit committee relationships
4	Strategic thinking	14	Creating a learning internal audit function
5	Time management	15	Change management
6	Presenting (small groups)	16	Developing outside contacts/networking
7	Leveraging others' expertise	17	Leadership (within the internal audit profession)
8	Developing rapport with senior executives	18	Coaching/mentoring
9	Negotiation	19	Presenting (public speaking)
10	High-pressure meetings		

Overall Results, Personal Skills and Capabilities – Three-Year Comparison

2015	2014	2013
Using/mastering new technology and applications	Presenting (public speaking)	Dealing with confrontation
Persuasion	Negotiation	Negotiation
Developing other board committee relationships		Persuasion
Strategic thinking	Persuasion	High-pressure meetings
Time management	Using/mastering new technology and applications	Presenting (public speaking)
	Dealing with confrontation	Strategic thinking
	Time management	
	Developing other board committee relationships	Developing other board committee relationships
		Using/mastering new technology and applications
	Developing outside contacts/ networking	Leadership (within the IA profession)
		Time management

Focus on Results by Company Size

Company Size Results, Personal Skills and Capabilities

Small ‹ US$1B	Medium US$1B-9B	Large › US$10B
Using/mastering new technology and applications	Using/mastering new technology and applications	Developing other board committee relationships
Persuasion	Time management	Persuasion
Leveraging others' expertise	Developing other board committee relationships	Negotiation
Developing rapport with senior executives	Persuasion	Presenting (small groups)
Strategic thinking	Strategic thinking	Developing rapport with senior executives
		Using/mastering new technology and applications

Focus on Chief Audit Executives

The findings from CAEs mirror the overall response. It is noteworthy that using/mastering new technology and applications figures as a top priority for CAEs as well as all respondents.

CAE Results, Personal Skills and Capabilities

"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Using/mastering new technology and applications	3.6
2 (tie)	Developing other board committee relationships	3.5
	Persuasion	3.8
4	Strategic thinking	3.9
5	Leveraging others' expertise	3.7

Key Questions for CAEs

- Is internal audit's approach to leadership development and training sufficient in light of the pressures, priorities and changes influencing the function?
- What is the full range of training methods (both formal and informal) internal audit can deploy to help staff master new auditing technologies?
- What signals are you, as CAE, sending to the rest of the function based on your personal approach to continuous learning, strengthening your professional networks, cultivating board relationships and skills development?
- What types of assignments (e.g., presenting to the board) might help future internal audit leaders develop the strategic thinking and presentation skills they need to excel?
- What is the current state of internal audit talent? What is the desired state? What is the plan for addressing gaps?

CAE Results, Personal Skills and Capabilities – Three-Year Comparison

2015	2014	2013
Using/mastering new technology and applications	Presenting (public speaking)	Dealing with confrontation
Developing other board committee relationships	Developing other board committee relationships	Developing other board committee relationships
Persuasion	Using/mastering new technology and applications	
Strategic thinking	Dealing with confrontation	Developing outside contacts/ networking
Leveraging others' expertise	Persuasion	Negotiation
	Developing outside contacts/ networking	Using/mastering new technology and applications
	Negotiation	Time management
		Persuasion
		Strategic thinking

> "IN A CHANGING ENVIRONMENT, WHILE CURRENT COMPETENCY MAY BE HIGH, THERE REMAINS A CONSTANT NEED TO IMPROVE."
>
> – Director of auditing, large manufacturing company

Methodology and Demographics

More than 800 respondents (n = 802) completed questionnaires for Protiviti's Internal Audit Capabilities and Needs Survey, which was conducted in the fourth quarter of 2014.

The survey consisted of a series of questions grouped into four divisions:

- Cybersecurity and the Audit Process
- General Technical Knowledge
- Audit Process Knowledge
- Personal Skills and Capabilities

Participants were asked to assess their skills and competency by responding to questions concerning nearly 200 topic areas. Respondents from the manufacturing, U.S. financial services and U.S. healthcare industries were also asked to assess industry-specific skills (these findings are available upon request). The purpose of this annual survey is to elicit responses that will illuminate the current perceived levels of competency in the many skills necessary to today's internal auditors, and to determine which knowledge areas require the most improvement.

Survey participants also were asked to provide demographic information about the nature, size and location of their businesses, and their titles or positions within the internal audit department. These details were used to help determine whether there were distinct capabilities and needs among different sizes and sectors of business or among individuals with different levels of seniority within the internal audit profession. All demographic information was provided voluntarily by respondents.

Position

Chief Audit Executive	18%
Director of Auditing	12%
IT Audit Director	1%
Audit Manager	23%
IT Audit Manager	5%
Audit Staff	23%
IT Audit Staff	7%
Corporate Management	2%
Other	9%

Size of Organization (by Gross Annual Revenue)

$20 billion or greater	10%
$10 billion - $19.99 billion	9%
$5 billion - $9.99 billion	11%
$1 billion - $4.99 billion	30%
$500 million - $999.99 million	13%
$100 million - $499.99 million	15%
Less than $100 million	12%

Industry

Financial Services (U.S.)	18%
Government/Education/Not-for-profit	14%
Manufacturing	11%
Insurance (excluding healthcare payer)	7%
Energy	6%
Technology	6%
Healthcare (U.S.) – Provider	5%
Retail	5%
Financial Services (Non-U.S.)	4%
Services	4%
CPA/Public Accounting/Consulting Firm	3%
Distribution	3%
Healthcare (U.S.) – Payer	3%
Hospitality	2%
Real Estate	2%
Telecommunications	2%
Utilities	2%
Other	3%

Certification

Certified Public Accountant (CPA)/Chartered Accountant (CA)	25%
Certified Internal Auditor (CIA)	23%
Certified Information Systems Auditor (CISA)	14%
Certification in Risk Management Assurance (CRMA)	9%
Certified Fraud Examiner (CFE)	8%
Certified Financial Services Auditor (CFSA)	2%
Certified Information Technology Professional (CITP)	1%
Certified Government Auditing Professional (CGAP)	1%

Type of Organization

Public	49%
Private	26%
Not-for-profit	12%
Government	10%
Other	3%

Organization Headquarters

North America	89%
Asia/Pacific	4%
Europe	4%
Middle East	2%
Latin America	1%

About Protiviti

Protiviti (**www.protiviti.com**) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 40 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is proud to be a Principal Partner of The IIA. More than 700 Protiviti professionals are members of The IIA and are actively involved with local, national and international IIA leaders to provide thought leadership, speakers, best practices, training and other resources that develop and promote the internal audit profession.

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.

Internal Audit and Financial Advisory

We work with audit executives, management and audit committees at companies of virtually any size, public or private, to assist them with their internal audit activities. This can include starting and running the activity for them on a fully outsourced basis or working with an existing internal audit function to supplement their team when they lack adequate staff or skills. Protiviti professionals have assisted hundreds of companies in establishing first-year Sarbanes-Oxley compliance programs as well as ongoing compliance. We help organizations transition to a process-based approach for financial control compliance, identifying effective ways to appropriately reduce effort through better risk assessment, scoping and use of technology, thus reducing the cost of compliance. Reporting directly to the board, audit committee or management, as desired, we have completed hundreds of discrete, focused financial and internal control reviews and control investigations, either as part of a formal internal audit activity or apart from it.

One of the key features about Protiviti is that we are not an audit/accounting firm, thus there is never an independence issue in the work we do for clients. Protiviti is able to use all of our consultants to work on internal audit projects – this allows us at any time to bring in our best experts in various functional and process areas. In addition, we can conduct an independent review of a company's internal audit function – such a review is called for every five years under standards from The IIA.

Among the services we provide are:

- Internal Audit Outsourcing and Co-Sourcing
- Financial Control and Sarbanes-Oxley Compliance
- Internal Audit Quality Assurance Reviews and Transformation
- Audit Committee Advisory

For more information about Protiviti's Internal Audit and Financial Advisory solutions, please contact:

Brian Christensen
Executive Vice President – Global Internal Audit
+1.602.273.8020
brian.christensen@protiviti.com

Protiviti Internal Audit and Financial Advisory Practice – Contact Information

Brian Christensen
Executive Vice President – Global Internal Audit
+1.602.273.8020
brian.christensen@protiviti.com

AUSTRALIA

Garran Duncan
+61.3.9948.1205
garran.duncan@protiviti.com.au

BELGIUM

Jaap Gerkes
+31.6.1131.0156
jaap.gerkes@protiviti.nl

BRAZIL

Raul Silva
+55.11.2198.4200
raul.silva@protivitiglobal.com.br

CANADA

Ram Balakrishnan
+1.647.288.8525
ram.balakrishnan@protiviti.com

CHINA (HONG KONG AND MAINLAND CHINA)

Albert Lee
+852.2238.0499
albert.lee@protiviti.com

FRANCE

Bernard Drui
+33.1.42.96.22.77
b.drui@protiviti.fr

GERMANY

Michael Klinger
+49.69.963.768.155
michael.klinger@protiviti.de

INDIA

Sachin Tayal
+91.98.1199.9076
sachin.tayal@protivitiglobal.in

ITALY

Alberto Carnevale
+39.02.6550.6301
alberto.carnevale@protiviti.it

JAPAN

Yasumi Taniguchi
+81.3.5219.6600
yasumi.taniguchi@protiviti.jp

MEXICO

Roberto Abad
+52.55.5342.9100
roberto.abad@protivitiglobal.com.mx

MIDDLE EAST

Manoj Kabra
+965.2295.7700
manoj.kabra@protivitiglobal.com.kw

THE NETHERLANDS

Jaap Gerkes
+31.6.1131.0156
jaap.gerkes@protiviti.nl

SINGAPORE

Sidney Lim
+65.6220.6066
sidney.lim@protiviti.com

SOUTH AFRICA

Fana Manana
+27.11.231.0600
fanam@sng.za.com

UNITED KINGDOM

Lindsay Dart
+44.207.389.0448
lindsay.dart@protiviti.co.uk

UNITED STATES

Brian Christensen
+1.602.273.8020
brian.christensen@protiviti.com

THE AMERICAS

UNITED STATES

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*

Buenos Aires

BRAZIL*

Rio de Janeiro
São Paulo

CANADA

Kitchener-Waterloo
Toronto

CHILE*

Santiago

MEXICO*

Mexico City

PERU*

Lima

VENEZUELA*

Caracas

ASIA-PACIFIC

AUSTRALIA

Brisbane
Canberra
Melbourne
Perth
Sydney

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*

Bangalore
Mumbai
New Delhi

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

* Protiviti Member Firm

EUROPE/MIDDLE EAST/AFRICA

FRANCE

Paris

GERMANY

Frankfurt
Munich

ITALY

Milan
Rome
Turin

THE NETHERLANDS

Amsterdam

UNITED KINGDOM

London

BAHRAIN*

Manama

KUWAIT*

Kuwait City

OMAN*

Muscat

QATAR*

Doha

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

SOUTH AFRICA*

Johannesburg

protiviti®
Risk & Business Consulting.
Internal Audit.

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