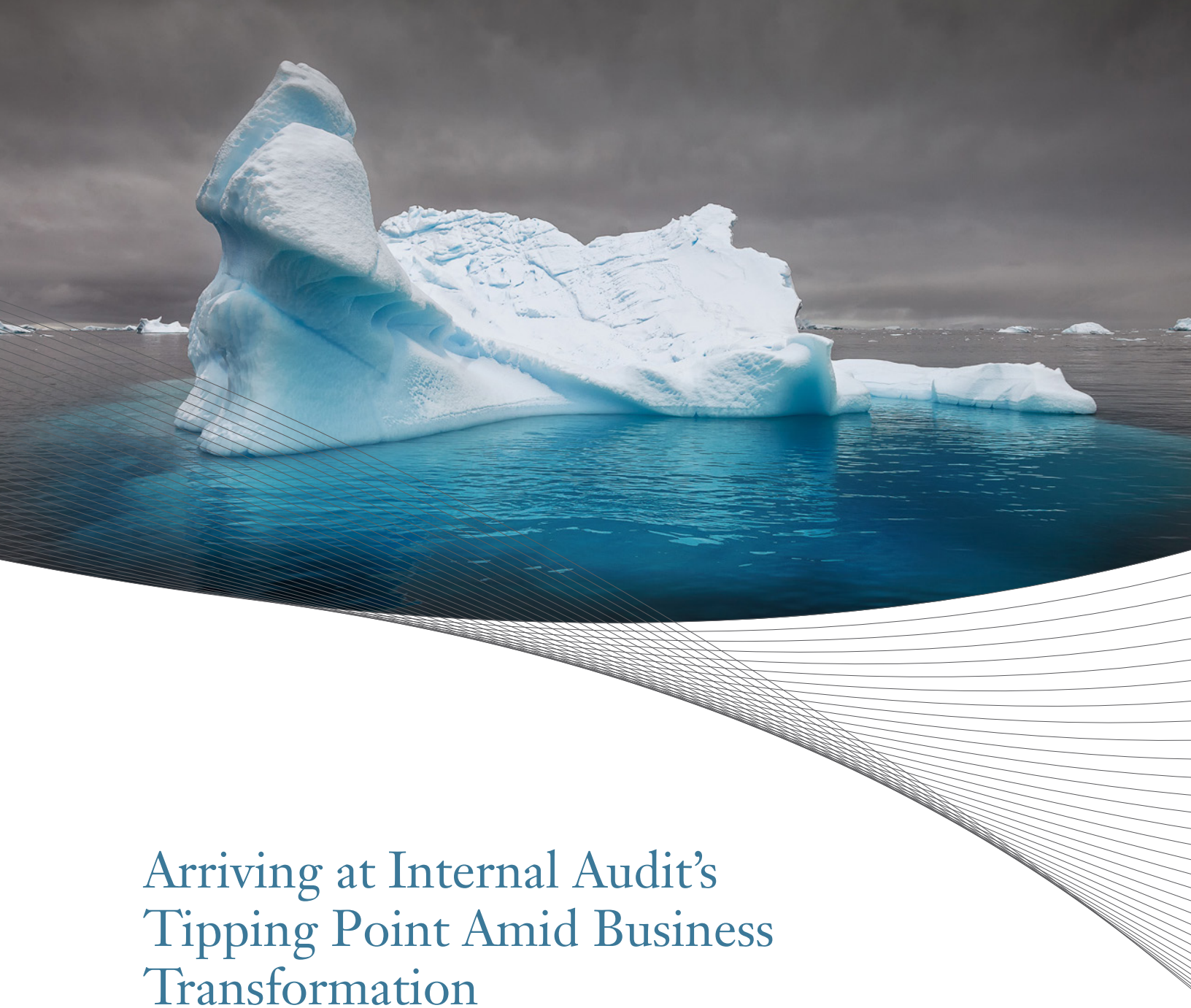


Arriving at Internal Audit's Tipping Point Amid Business Transformation

Assessing the Results of the 2016 Internal Audit Capabilities and Needs Survey – and a Look at Key Trends over the Past Decade

protiviti®
Risk & Business Consulting.
Internal Audit.

Powerful Insights. Proven Delivery.®

"The tipping point is that magic moment when an idea, trend, or social behavior crosses a threshold, tips, and spreads like wildfire."

– Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference*[1]

Introduction

How is your internal audit function evolving?

This question contains a subtle yet blunt challenge: Standing pat will not suffice. Internal audit stakeholders in the C-suite, on the board of directors and throughout the organization rely greatly on their internal audit functions to provide assurance- and compliance-related activities. But more and more, these contributions represent just the tip of the iceberg. Amid ongoing business transformation, stakeholders seek more input from their internal audit groups, including but not limited to risks tied to long-term strategy or a catastrophic cybersecurity breach that may be lurking just beneath the surface.

From a strategic perspective, other hazards loom on the horizon, including the risks associated with digital transformation, mobile technology and ongoing regulatory changes. And who knows the depth of data-protection risks that lurk with the rising adoption of the Internet of Things (IoT)? These trends offer massive growth opportunities, but they also present threats that must be rigorously identified, assessed and monitored so that organizations can face the future with confidence.

In the 10th year of our Internal Audit Capabilities and Needs Survey, we believe internal audit has arrived at a tipping point. The issue is no longer whether or not your function is evolving, but rather how quickly and effectively it is transforming for the future toward a more strategic, collaborative and data-driven mode of operation while maintaining the highest quality of performance.

Our key findings:

- **The strength of cybersecurity measures hinges on board engagement and inclusion in the audit plan –** Cybersecurity is not an IT issue – it is a business risk requiring a comprehensive, risk-based approach to manage. The most effective cybersecurity audit capabilities are supported in organizations where the board is highly engaged in information security risks and where cybersecurity risk is included in the audit plan.
- **Cybersecurity risk is becoming a fixture in the annual audit plan –** Nearly three out of four organizations are evaluating cybersecurity risk as part of the annual audit plan, compared to just half of organizations in 2015.
- **Notable audit priorities include mobile applications, cloud computing, IT standards and the Internet of Things –** Technology issues dominate the priority list for internal auditors, from emerging technologies and trends to IT auditing standards.
- **It's time to move forward with data analysis and technology-enabled auditing capabilities –** Internal audit continues to view data analytics and technology-enabled auditing as significant priorities, but after a decade of stagnant growth, we're at a tipping point where more progress is needed.

In celebrating the 10th anniversary of our study, we deeply appreciate the more than 1,300 chief audit executives and internal audit professionals who participated this year, and the thousands who participated in prior years. We also appreciate the outstanding global leadership provided by The Institute of Internal Auditors (IIA) in advancing the strategic role of internal audit in business today.

[1] © 2000, Little, Brown and Company.

Cybersecurity and the Audit Process

Key Findings

- Companies with the most effective audit capabilities around cybersecurity include this risk in the annual audit plan and have a board of directors that is highly engaged in information security risk.
- Nearly three out of four internal audit functions include evaluating and auditing cybersecurity risk as part of their audit plan – a significant improvement compared to our 2015 results.
- Brand and reputation damage, data security (company information) and data leakage (employee personal information) represent the greatest cybersecurity risks.
- A lack of resources/skills as well as a lack of software tools are hindering organizations' efforts to address specific areas of cybersecurity sufficiently.

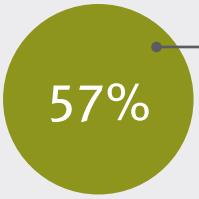
Cybersecurity has graduated from an IT risk to a strategic business risk and an issue now addressed regularly by the board of directors. The good news is that according to our survey results, many organizations, and especially internal audit functions, have notched significant improvements in numerous facets of their cybersecurity capability. The most notable sign of progress: 73 percent of organizations now include cybersecurity risk in the annual audit plan, compared to 53 percent in our 2015 survey.

Nevertheless, our results suggest substantial progress is needed if organizations are to avoid the terrible news that they have been struck by a crippling cyberattack. The fact is that when it comes to cybersecurity, the risks in view may only represent the tip of the iceberg.

To focus on what may be lingering below the surface, cybersecurity risk management strategies not only should be in place, but they also must be effective. Boards should not only be aware of cybersecurity risks, but they also should be engaged, at least at a high level, with the organization's cybersecurity measures. And internal audit should integrate cybersecurity into its daily activities as well as its annual audit plan.

Similar to last year, our results show that two differentiators – a high level of board engagement in information security and cybersecurity's inclusion in the current audit plan – are key success factors in addressing cybersecurity risk effectively.

KEY FACT



Percentage of companies that have received inquiries from customers, clients and/or insurance providers about the organization's state of cybersecurity

Cybersecurity Top Performers – High Board Engagement, Audit Plan Inclusion

In our results, we have found two critical success factors in establishing and maintaining effective cybersecurity measures:

1. **A high level of engagement by the board of directors in information security risks**
2. **Evaluating cybersecurity risk as part of the current audit plan**

Organizations with at least one of these success factors in place, which we identify throughout our report as "top performers," are significantly more likely to have a stronger risk posture to combat cyberthreats. Our results and accompanying commentary point out that while many organizations are making progress in addressing these issues, they still have a way to go in their journey to navigate increasingly treacherous cybersecurity waters.

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

	2016	2015
High engagement and level of understanding by the board	24%	30%
Medium engagement and level of understanding by the board	37%	41%
Low engagement and level of understanding by the board	24%	14%
Don't know	15%	15%

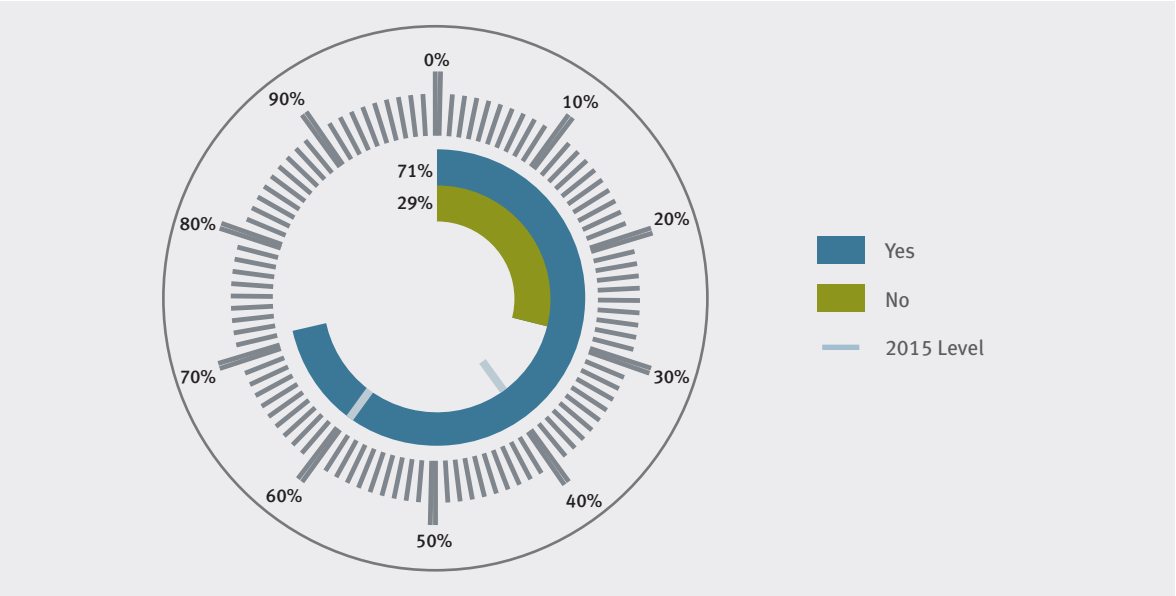
Is evaluating and auditing cybersecurity risk part of your audit plan?

	2016	2015
Yes, it is included in our current year audit plan	73%	53%
No, but it will be included in next year's audit plan	16%	27%
We have no plans to include it in the audit plan	11%	20%

The results show a substantial year-over-year jump in the number of organizations that now include cybersecurity risk in the annual audit plan. This undoubtedly reflects higher levels of interest and concerns among organizations about the cyberthreats they now encounter daily. In addition, many organizations likely are being influenced by their external auditors placing increased scrutiny on management's cybersecurity program. This is being driven by the current cyberthreat environment along with SEC disclosure obligations issued in 2011 relating to cybersecurity risks and cyber incidents, which set the stage for the market developments we are witnessing today.[2]

[2] CF Disclosure Guidance: Topic No. 2, "Cybersecurity," Division of Corporation Finance, U.S. Securities and Exchange Commission, October 13, 2011, www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

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



"The audit process must exist within a context, and that context is best provided through the establishment of a meaningful, business-focused NIST target profile."

– Chief audit executive, small financial services company, North America

Current State of Cybersecurity – An Internal Audit Perspective

There is a clear need among most internal audit groups to strengthen their ability to identify, assess and mitigate cybersecurity risk to an acceptable level. But these capabilities are much stronger for top-performing organizations, particularly with regard to the level of board engagement in information security risks. While there is less of a difference in the results among companies that do and do not include cybersecurity risk in their annual audit plan, note that many more internal audit groups are now formally assessing this risk (see page 2). It is likely that, for more companies, this is bringing greater clarity about cybersecurity risk and areas that require improvement.

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

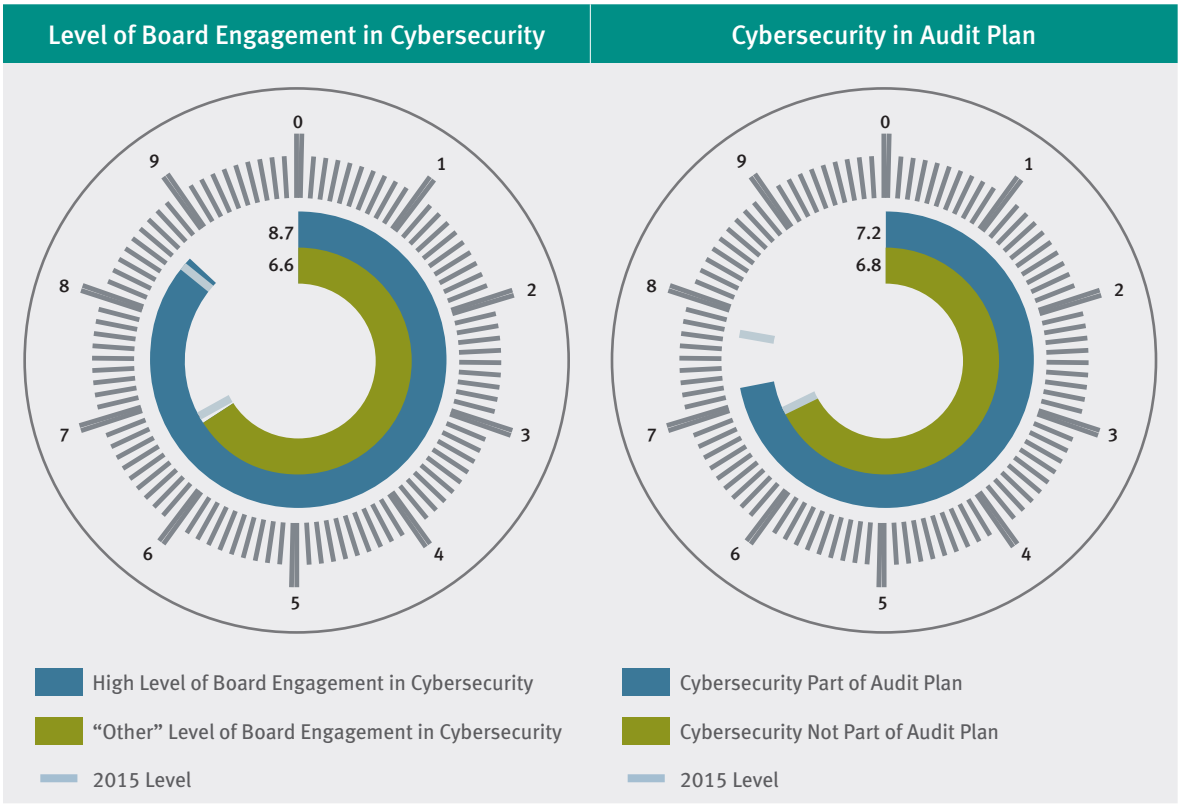
	High Level of Board Engagement		"Other" Level of Board Engagement		Cybersecurity Part of Audit Plan		Cybersecurity Not Part of Audit Plan	
	2016	2015	2016	2015	2016	2015	2016	2015
Identifying	57%	47%	19%	19%	30%	35%	24%	20%
Assessing	55%	43%	16%	19%	27%	31%	18%	21%
Mitigating	45%	39%	12%	15%	22%	26%	15%	18%

"[We are] concerned that people consider cybersecurity and information security to be the same thing and, therefore, gaps in controls are overlooked."

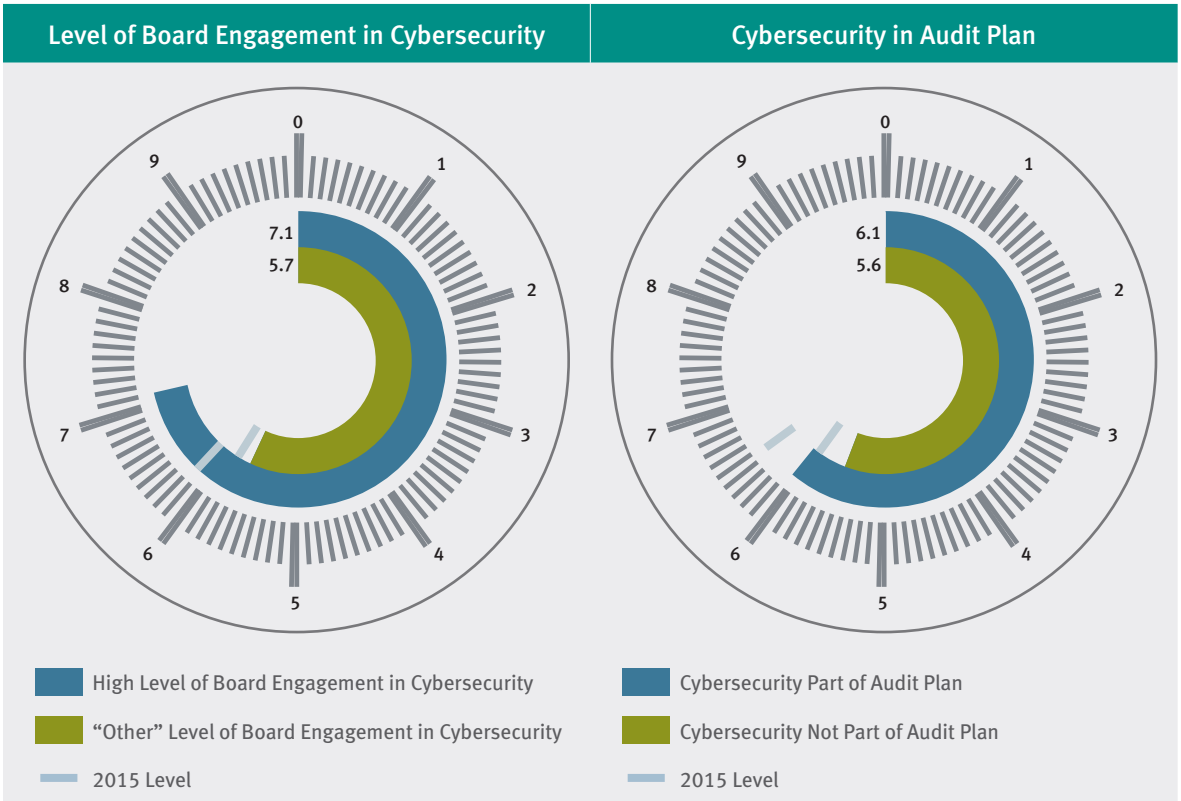
– Chief audit executive, midsize insurance company, North America

Once again, there is relatively strong awareness about information security exposures, particularly among top-performing companies. Similar to last year's findings, there are lower levels of confidence in the ability to prevent a cybersecurity breach by an employee or business partner (see below and following pages).

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).

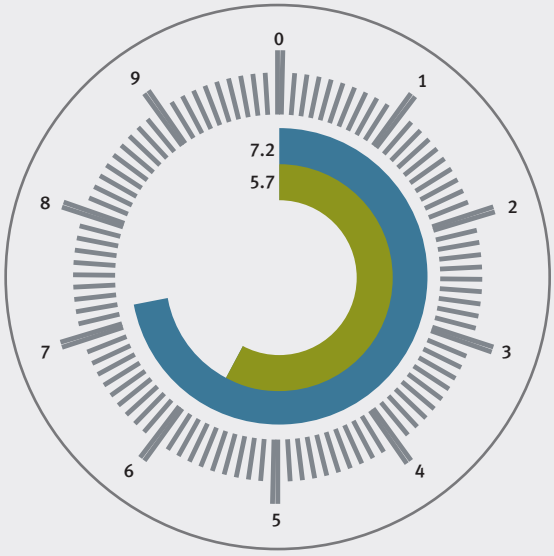


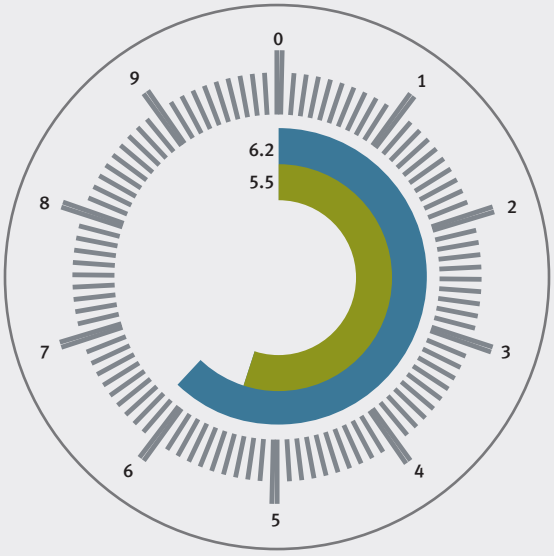
"[Cybersecurity] is a work in process. As the company readjusts its strategy to the ever-emerging changing landscape, so much the response in our audit function/plan."

– IT audit director, large healthcare provider, North America

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 a targeted external attack by a well-funded attacker.

Level of Board Engagement in Cybersecurity	Cybersecurity in Audit Plan





High Level of Board Engagement in Cybersecurity

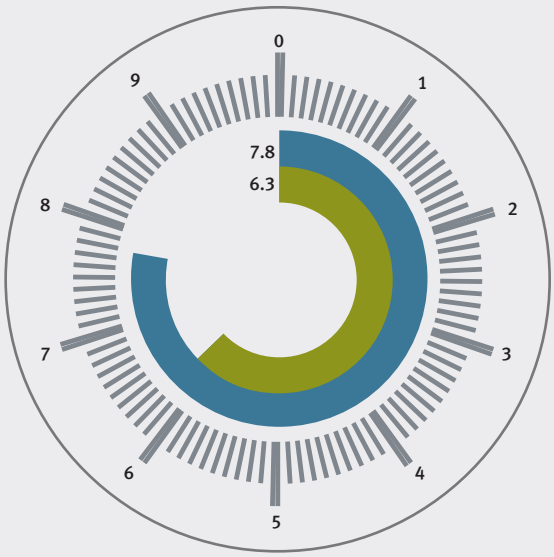
"Other" Level of Board Engagement in Cybersecurity

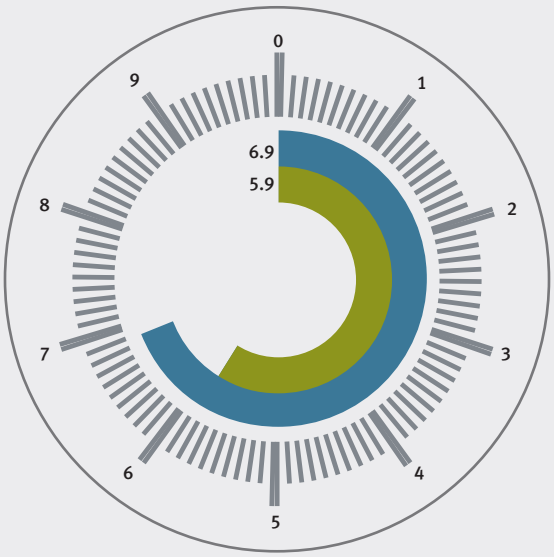
Cybersecurity Part of Audit Plan

Cybersecurity Not Part of Audit Plan

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 monitor, detect and escalate potential security incidents by a well-funded attacker.

Level of Board Engagement in Cybersecurity	Cybersecurity in Audit Plan





High Level of Board Engagement in Cybersecurity

"Other" Level of Board Engagement in Cybersecurity

Cybersecurity Part of Audit Plan

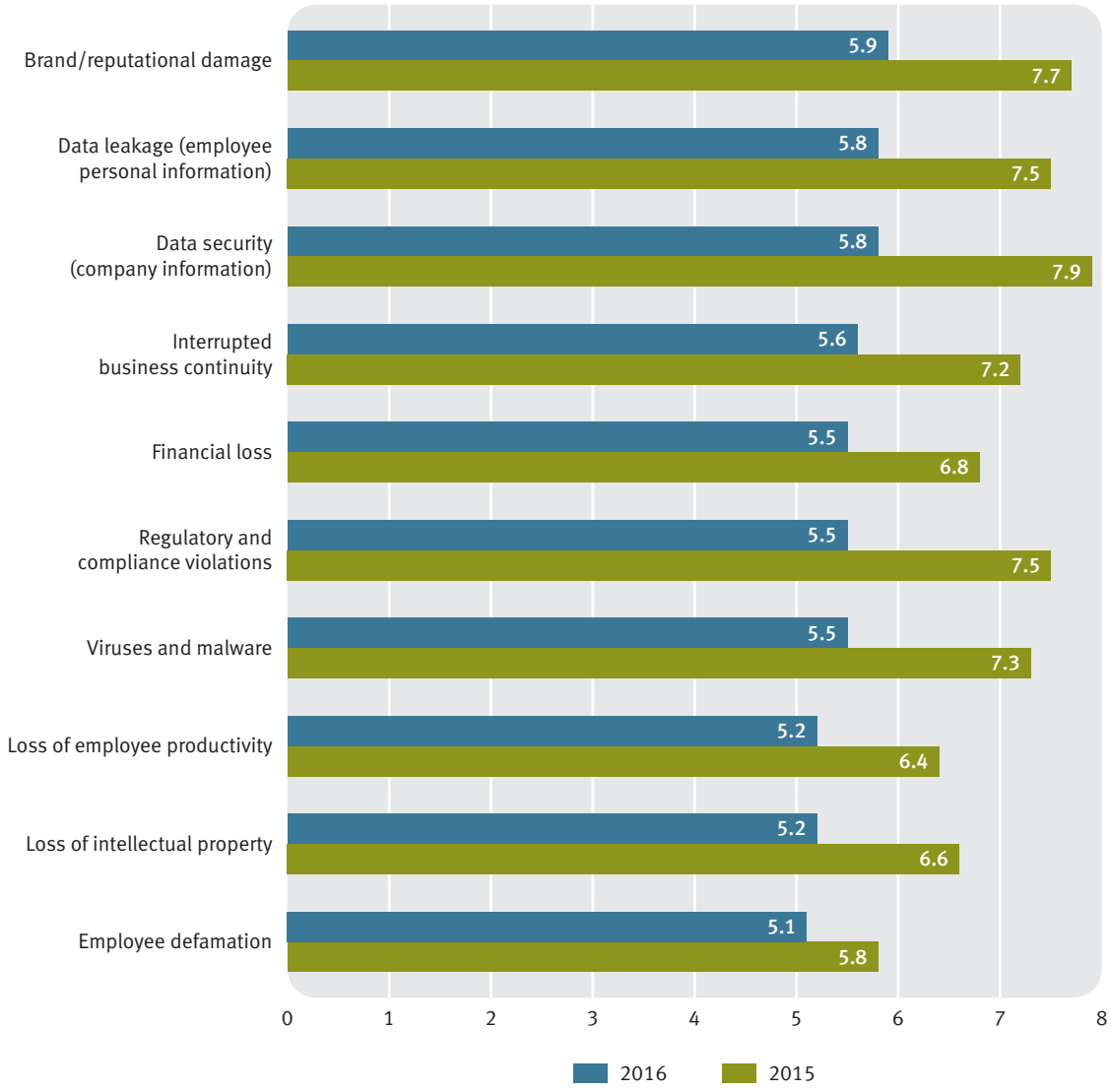
Cybersecurity Not Part of Audit Plan

Brand and reputation damage, data leakage and data security are viewed to pose the most significant levels of cybersecurity risk. In terms of the value derived from addressing cybersecurity risks, organizations view their ability to identify issues, risk or control problems early to be most important, along with monitoring reputation risk and improving operational performance (which jumped significantly compared to our prior year results).

Across the board, the perceived level of cybersecurity risk for different areas dropped compared to our 2015 findings. One possible explanation is that, given widespread market and media coverage, organizations may feel more educated and aware of cybersecurity risks and issues than they did 12 months ago. This may bring more comfort and confidence in the ability to address them. But it's important to consider that education and awareness could create a false sense of confidence about the organization's ability to manage these risks: Knowing about them does not translate into an ability to manage them effectively. These issues must remain on the organization's radar, and internal auditors should remain objective and skeptical in their risk assessments – even one security weakness lurking beneath the surface could have extensive consequences.

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

	2016	2015
Earlier identification of issues, risk or control problems	33%	40%
Monitor reputation risk	22%	15%
Improved operational performance	16%	5%
Overall business strategy	9%	11%
Regulatory compliance	9%	16%
Validation of control effectiveness or failure	6%	10%
Cost recovery/improvement	4%	3%
Other	1%	0%

"[Cybersecurity] continues to be a focus area for the board, although they recognize that our risk profile is not as high as other companies. As such, the board's response has been more measured and not overly reactive to current news and trends."

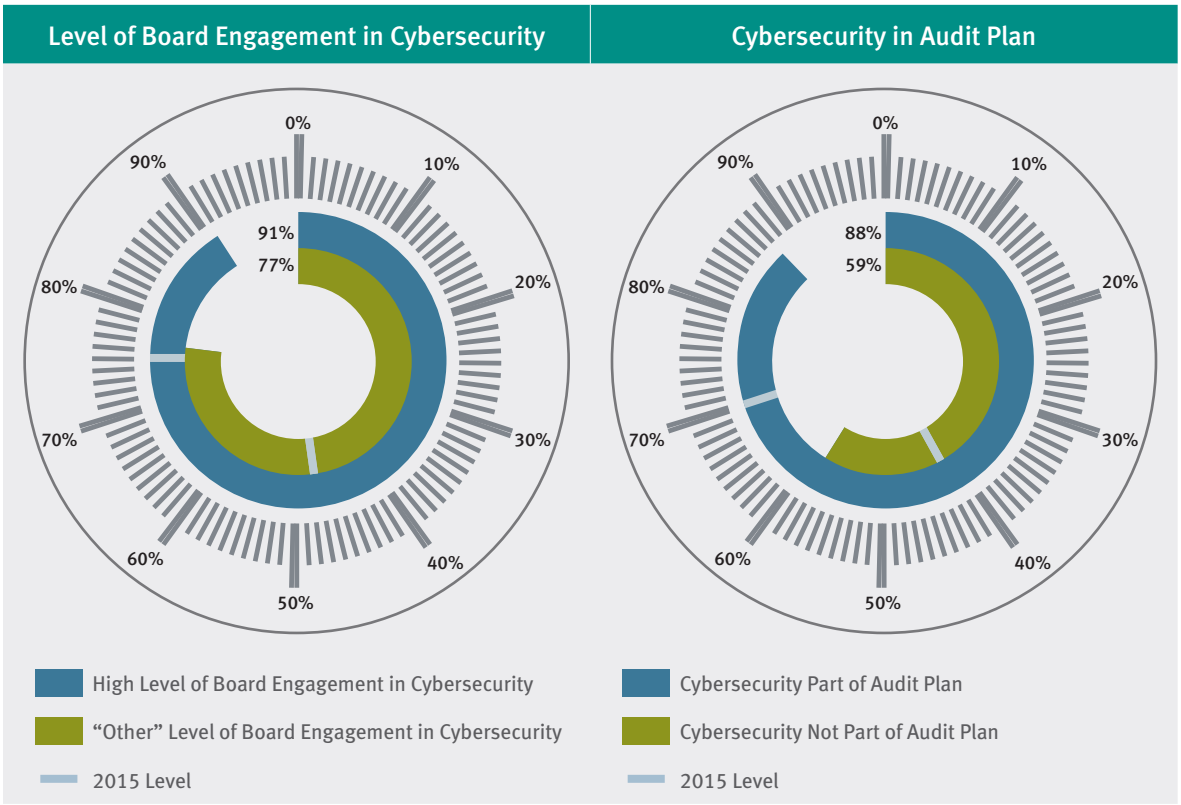
– Chief audit executive, midsize manufacturing company, North America

Assessing Cybersecurity Best Practices

Overall, four out of five organizations have a cybersecurity risk strategy in place, and three out of four have a cybersecurity policy in place. These findings represent significant increases compared to our 2015 survey results. There also remains a noticeable gap between "top performers" and other organizations.

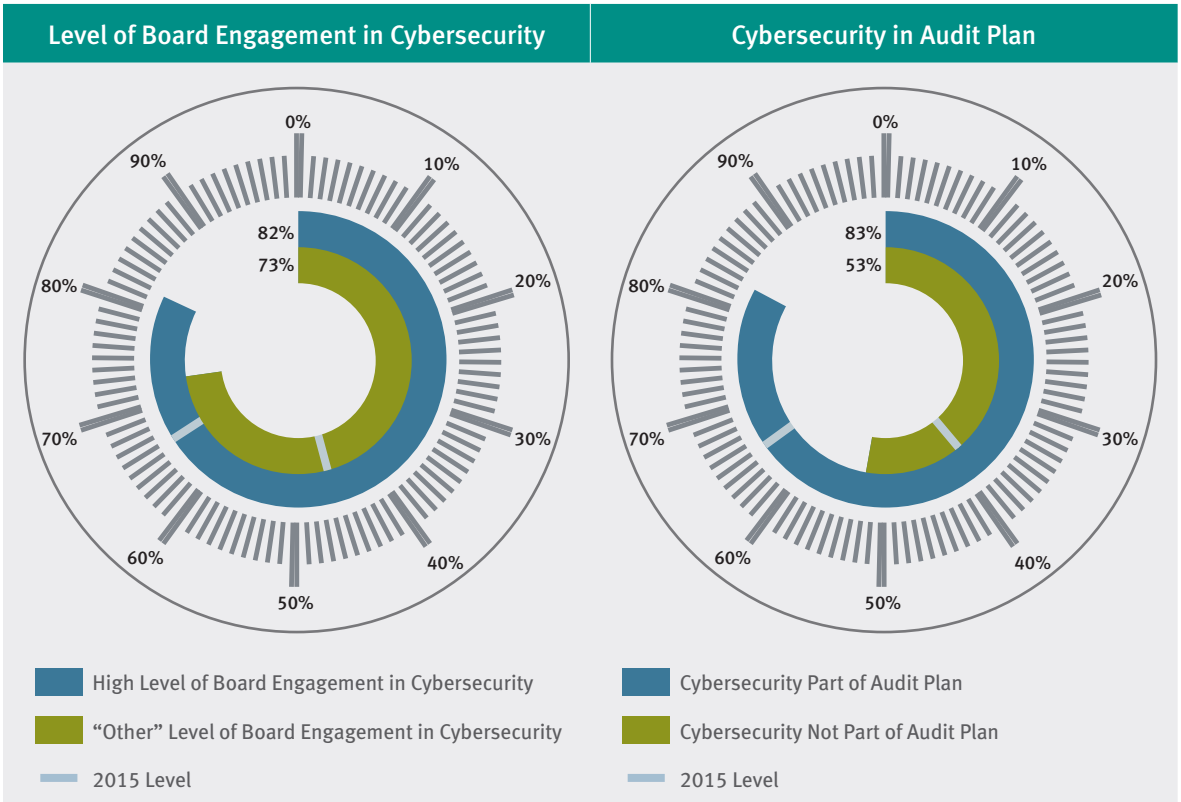
Keep in mind that widespread communications about cybersecurity and cyberthreats are likely driving many organizations to create such strategies and policies. These are positive steps but only the first ones if organizations hope to navigate these treacherous waters successfully. Strategies and policies alone are not a panacea for cybersecurity risk – they must be accompanied by effective communication and application of them throughout the organization.

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



** Shown: Percentages of "Yes" responses*

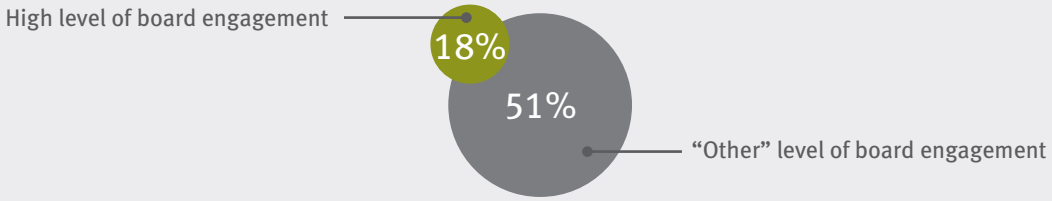
Does your organization have a cybersecurity risk policy in place?*



** Shown: Percentages of "Yes" responses*

KEY FACTS

Percentage of organizations, by level of board engagement in information security risks, in which there are specific areas of cybersecurity risk that are not addressed sufficiently due to lack of software tools



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	
	2016	2015	2016	2015	2016	2015	2016	2015
Yes, it is addressed separately from the overall risk assessment process	28%	32%	46%	22%	50%	32%	23%	17%
Yes, it is addressed as part of the overall risk assessment process	68%	63%	42%	56%	47%	65%	48%	49%
No	4%	5%	12%	22%	3%	3%	29%	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	
	2016	2015	2016	2015	2016	2015	2016	2015
Audit committee	17%	17%	60%	43%	17%	28%	6%	12%
Company IT organization representatives	53%	33%	43%	47%	3%	17%	1%	3%
Executive management	25%	44%	62%	41%	12%	13%	1%	2%
External audit	11%	20%	56%	46%	26%	28%	7%	6%
Human resources	5%	69%	40%	27%	41%	3%	14%	1%
Internal audit/IT audit	38%	48%	28%	38%	32%	11%	2%	3%
Legal	16%	31%	30%	34%	47%	19%	7%	16%
Line of business executives	10%	4%	32%	27%	50%	44%	8%	25%
Management and/or process owners	14%	13%	38%	38%	43%	34%	5%	15%
Marketing/ PR/corporate communications	4%	4%	30%	23%	49%	43%	17%	30%
Risk management (separate from internal audit)	25%	18%	34%	38%	31%	32%	10%	12%
Third-party service provider	10%	13%	36%	35%	38%	28%	16%	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	
	2016	2015	2016	2015	2016	2015	2016	2015
Audit committee	86%	81%	73%	48%	81%	66%	60%	51%
Company IT organization representatives	98%	94%	96%	73%	97%	82%	94%	78%
Executive management	95%	91%	84%	81%	91%	86%	74%	83%
External audit	65%	81%	67%	58%	72%	67%	48%	63%
Human resources	51%	97%	43%	96%	52%	97%	20%	94%
Internal audit/IT audit	95%	93%	56%	82%	64%	94%	71%	73%
Legal	79%	85%	35%	55%	46%	70%	46%	57%
Line of business executives	78%	45%	30%	23%	43%	33%	38%	26%
Management and/or process owners	78%	64%	43%	44%	52%	55%	46%	44%
Marketing/ PR/corporate communications	53%	45%	28%	18%	36%	28%	27%	25%
Risk management (separate from internal audit)	83%	73%	50%	46%	58%	59%	58%	51%
Third-party service provider	64%	59%	40%	42%	46%	55%	45%	37%

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

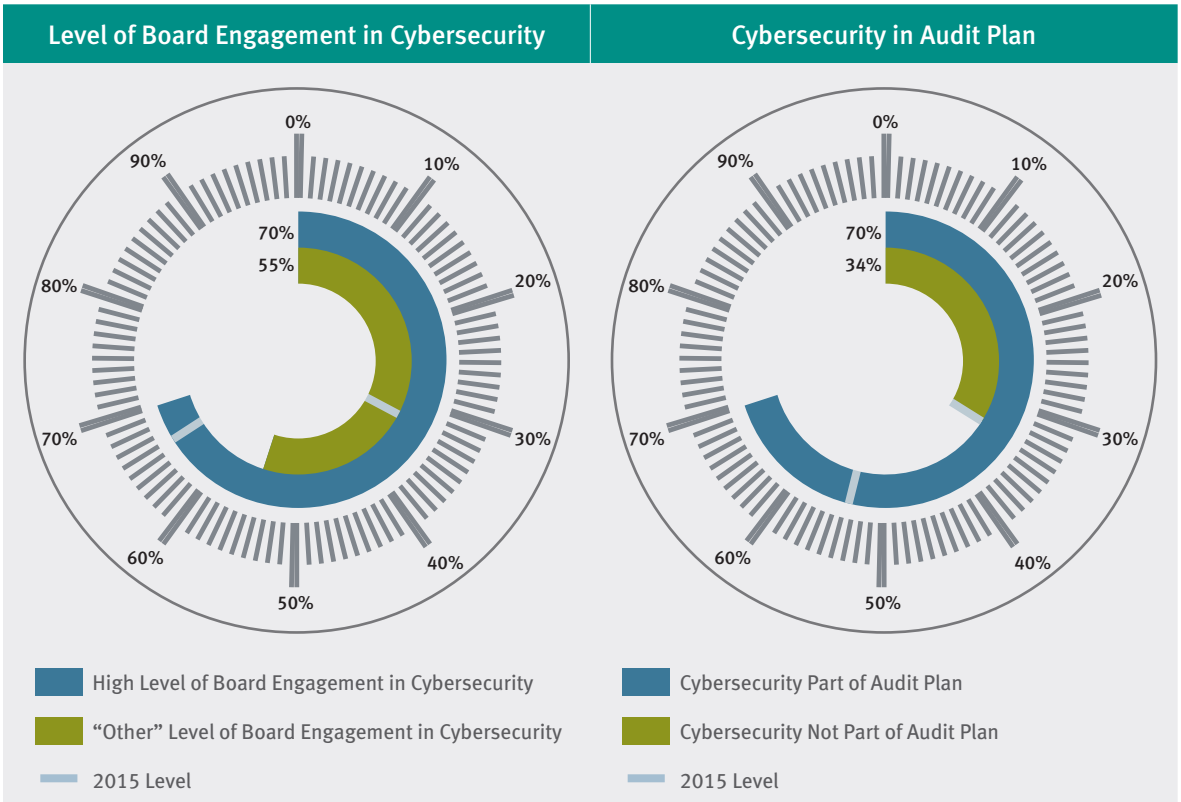
"Cybersecurity risk is an area that is still not well defined. We tend to focus on specific application, database, operating system and general controls, without consideration of how the overall strategy for assessing cyber risk affects the company as a whole."

– IT audit director, large construction/engineering company, North America

In a majority of organizations, the CIO regularly reports to the audit committee on cybersecurity and IT risks, in general. Notably, the numbers are higher for top-performing companies.[3]

Talent and technology tools represent fast-growing challenges for many organizations in their efforts to strengthen cybersecurity. Compared to our 2015 results, approximately twice as many respondents this year indicated their organizations are not able to address specific areas of cybersecurity risk sufficiently due to shortcomings in resources/skills or software tools.

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



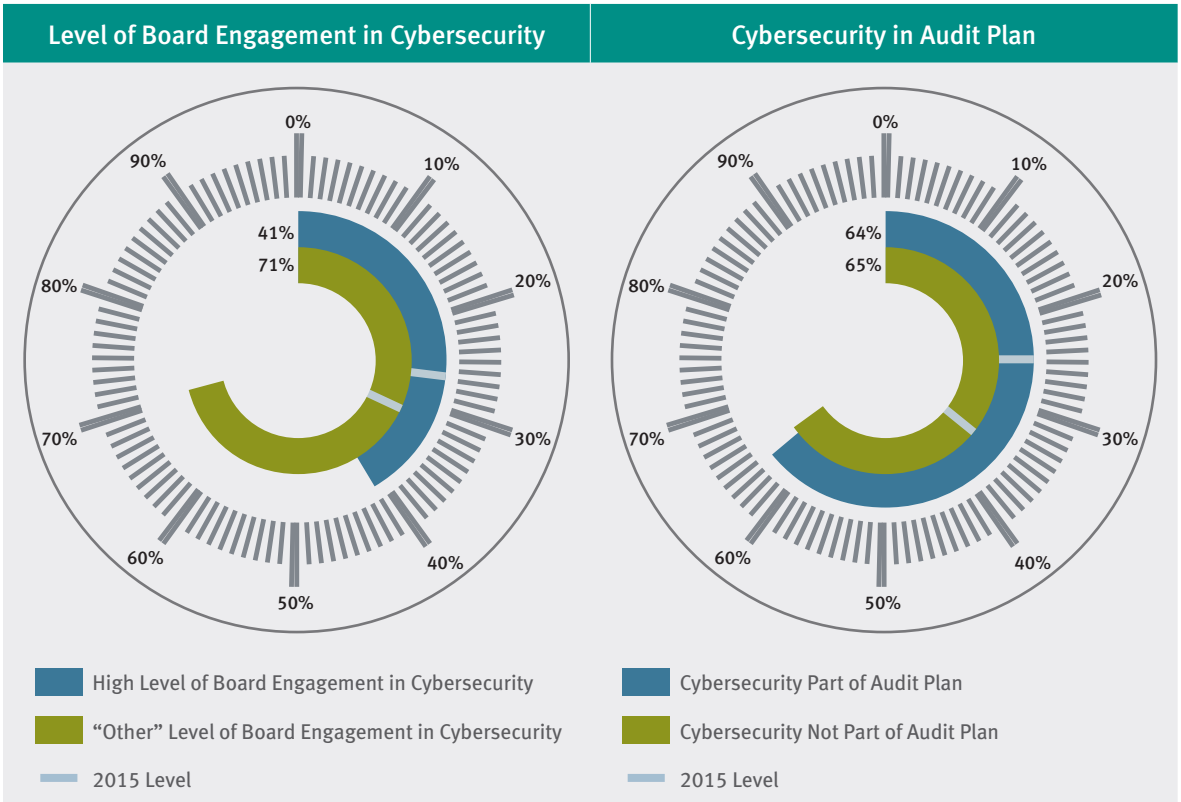
** Shown: Percentages of "Yes" responses*

"We are addressing cyber-risk management through a series of audits because I don't believe one audit could cover it all."

– Chief audit executive, large insurance company, North America

[3] For additional information on this topic, read Issue 67 of Protiviti's *Board Perspectives: Risk Oversight*, "Briefing the Board on IT Matters," May 2015, available at www.protiviti.com/board.

Are there specific areas of cybersecurity risk that you are not able to address sufficiently in your audit plan due to lack of resources/skills?*



** Shown: Percentages of "Yes" responses*

IF "YES": What steps have you taken to fill this gap?

	High Level of Board Engagement	"Other" Level of Board Engagement	Cybersecurity Part of Audit Plan	Cybersecurity Not Part of Audit Plan
Plans to bring in full-time professionals	11%	35%	41%	7%
Plans to bring in project/contract professionals	27%	26%	29%	19%
Plans to retain third-party firm to provide assistance	39%	19%	19%	30%
No specific plans currently in place	23%	20%	11%	44%

Ten Cybersecurity Action Items for CAEs and Internal Audit
1. Work with management and the board to develop a cybersecurity strategy and policy.
2. Identify and act on opportunities to improve the organization's ability to identify, assess and mitigate cybersecurity risk to an acceptable level.
3. Recognize that cybersecurity risk is not only external – assess and mitigate potential threats that could result from the actions of an employee or business partner.
4. Leverage relationships with the audit committee and board to (a) heighten awareness and knowledge of cyberthreats; and (b) ensure the board remains highly engaged with cybersecurity matters and up to date on the changing nature of cybersecurity risk.
5. Ensure cybersecurity risk is integrated formally into the audit plan.
6. Develop, and keep current, an understanding of how emerging technologies and trends are affecting the company and its cybersecurity risk profile.
7. Evaluate the organization's cybersecurity program against the NIST Cybersecurity Framework, recognizing that because the framework does not reach down to the control level, your cybersecurity program may require additional evaluations of ISO 27001 and 27002.
8. Seek out opportunities to communicate to management that with regard to cybersecurity, the strongest preventive capability requires a combination of human and technology security – a complementary blend of education, awareness, vigilance and technology tools.
9. Emphasize that cybersecurity monitoring and cyber-incident response should be 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 as well as a lack of supporting technology tools, either of which can impede efforts to manage cybersecurity risk effectively.

General Technical Knowledge

Key Findings

- Technology-related risks, and cybersecurity risks in particular, stand out among the priorities for internal auditors.
- Other key areas of focus for the coming year include ISO 27000, mobile applications and the NIST Cybersecurity Framework.
- Two new areas in this year's survey – the Internet of Things, and agile risk and compliance – also rank among this year's top internal audit priorities.
- Over the past decade, the most oft-cited priorities have a distinct IT focus.

Overall Results, General Technical Knowledge		
"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	ISO 27000 (information security)	2.4
2	Mobile applications	2.3
3	NIST Cybersecurity Framework	2.2
4	GTAG 16 – Data Analysis Technologies	2.5
5 (tie)	Internet of Things	2.6
	Agile risk and compliance	2.3

Commentary – Overall Findings

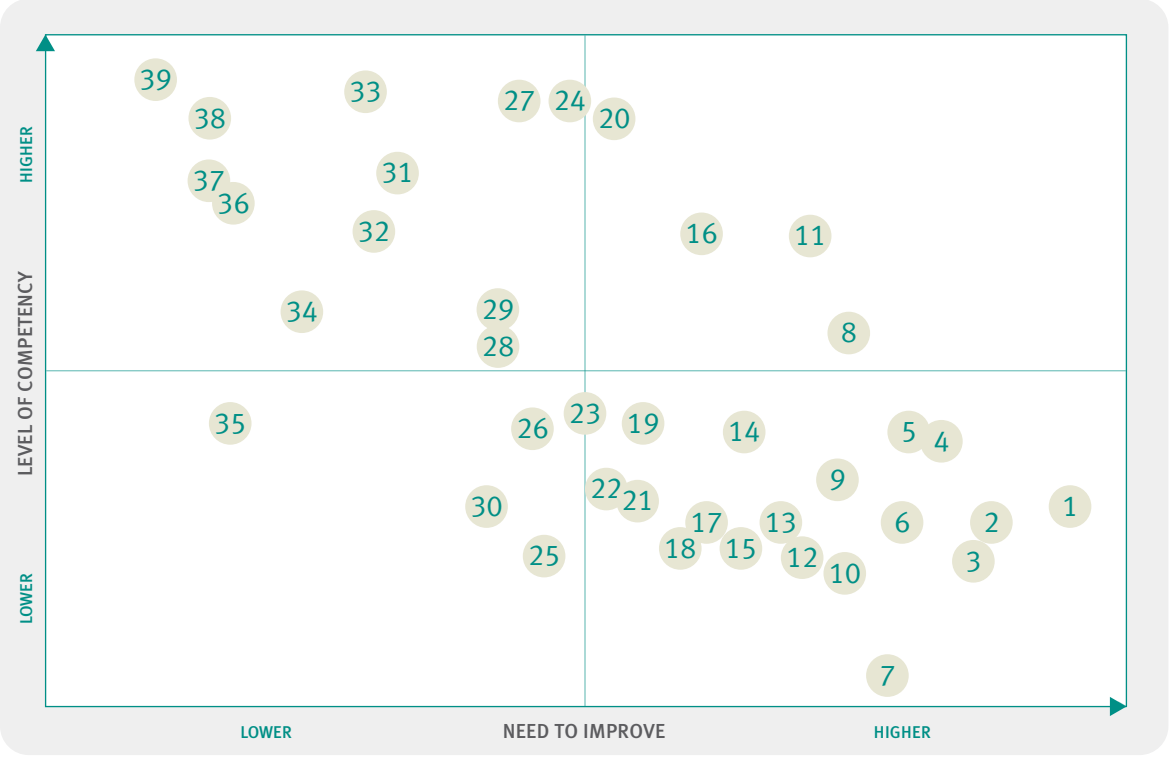
Respondents were asked to assess, on a scale of 1 to 5, their competency in 39 areas of technical knowledge important to internal audit, with "1" being the lowest level of competency and "5" being the highest. For each area, they were then asked to indicate whether they believe their level of knowledge is adequate or requires improvement, taking into account the circumstances of their organization and industry. (For the areas of knowledge under consideration, see page 19.) Figure 1 on the following page depicts a comparison of "Need to Improve" versus "Competency" ratings in a General Technical Knowledge landscape.

Not surprisingly, the top priorities identified this year all relate to IT risks (mobile applications, IOT), standards (ISO 27000 – information security) and directives (NIST and The IIA's GTAG 16 – Data Analysis Technologies). Technology issues are also prevalent in this year's top 10 priorities, which include big data/business intelligence and GTAG 17 – Auditing IT Governance.

Another top priority, agile risk and compliance, is related to technology on two counts. First, the rapid pace of technological change within organizations (e.g., the sudden spread of mobile technology among the workforce and the supply chain) gives rise to new risks, many of which must be integrated into internal audit's activities to help strengthen the enterprise's overall IT governance capability. Second, an agile risk and compliance capability is enabled by technology, such as data analysis and continuous monitoring (a top priority in the Audit Process Knowledge section that follows).

Internal Audit Action Items
• Understand the company's current strategic risks and anticipate what the top strategic risks will look like 12 months from now.
• Develop and strengthen collaborative relationships with stakeholders throughout the company to address a dynamic and comprehensive set of business risks proactively.
• With cybersecurity now a full-fledged business risk and a growing board of directors concern, recognize the strategic impact of the issue, collaborate with stakeholders throughout the company to evaluate and monitor its changing nature, and invest in the tools and expertise necessary to do so.
• Help ensure the company's approach to managing cybersecurity and other increasingly important technology (e.g., mobile, analytics, IoT) is comprehensive and risk-based.
• Ensure fraud detection and prevention activities remain sufficient given the technology, structural, strategic and workforce changes occurring throughout the organization.

Figure 1: General Technical Knowledge – Perceptual Map



Number	General Technical Knowledge	Number	General Technical Knowledge
1	ISO 27000 (information security)	21	The Guide to the Assessment of IT Risk (GAIT)
2	Mobile applications	22	Social media applications
3	NIST Cybersecurity Framework	23	COBIT
4	GTAG 16 – Data Analysis Technologies	24	2013 COSO Internal Control Framework – Information and Communication
5	Internet of Things	25	Six Sigma
6	Agile risk and compliance	26	Functional Reporting Interpretation (IIA Standard 1110)
7	ISO 14000 (environmental management)	27	2013 COSO Internal Control Framework – Risk Assessment
8	Country-specific enterprise risk management framework	28	Corporate social responsibility
9	Big data/business intelligence	29	Revenue Recognition Standard (Financial Accounting Standards Board (FASB) Accounting Standards Update No. 2014-09)
10	GTAG 17 – Auditing IT Governance	30	Lease accounting standard
11	Assurance around outsourced service providers	31	COSO Enterprise Risk Management Framework
12	ISO 31000 (risk management)	32	Fraud risk management
13	Cloud computing accounting standard	33	2013 COSO Internal Control Framework – Control Environment
14	International Financial Reporting Standards (IFRS)	34	Overall Opinions (IIA Standard 2450)
15	Cloud computing	35	Foreign Corrupt Practices Act (FCPA)
16	Reporting on Controls at a Service Organization – SSAE 16/AU 324 (also known as SOC1 and SOC reports)	36	IIA International Professional Practices Framework (IPPF) (Updated)
17	ISO 9000 (quality management and quality assurance)	37	Audit Opinions and Conclusions (IIA Standards 2010.A2 and 2410.A1)
18	Business/digital transformation	38	2013 COSO Internal Control Framework – Monitoring Activities
19	Auditing corporate culture	39	2013 COSO Internal Control Framework – Control Activities
20	2013 COSO Internal Control Framework – Evaluation of “Presence, Functioning and Operating Together”		

Overall Results, General Technical Knowledge – 10-Year Trends

Rank	2016	2015	2014	2013	2012
1	ISO 27000 (information security)	GTAG 16 – Data Analysis Technologies	Mobile applications	Social media applications	Social media applications
2	Mobile applications	NIST Cybersecurity Framework	NIST Cybersecurity Framework	Recently enacted IIA Standard – Functional Reporting Interpretation (Standard 1110) Recently enacted IIA Standards – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)	Cloud computing
3	NIST Cybersecurity Framework	Mobile applications	Social media applications	GTAG 16 – Data Analysis Technologies Recently enacted IIA Standard – Overall Opinions (Standard 2450) Cloud computing	GTAG 13 – Fraud Prevention and Detection
4	GTAG 16 – Data Analysis Technologies	Practice Advisory 2320-4 – Continuous Assurance	Cloud computing	The Guide to the Assessment of IT Risk (GAIT) GTAG 13 – Fraud Prevention and Detection ISO 27000 (information security) COSO Internal Control Framework (DRAFT 2012 version)	Fraud risk management
5	Internet of Things Agile risk and compliance	The Guide to the Assessment of IT Risk (GAIT)	GTAG 16 – Data Analysis Technologies	Practice Guide – Assessing the Adequacy of Risk Management GTAG 6 – Managing and Auditing IT Vulnerabilities Fraud risk management	GTAG 16 – Data Analysis Technologies

Three of the four areas most frequently ranked as top priorities in the past 10 years have a distinct IT focus – ISO 27000 (information security), GTAG 16 – Data Analysis Technologies, and the Guide to the Assessment of IT Risk (GAIT). The other, fraud risk management, requires an increasing level of technology and analysis tools to perform effectively.

2011	2010	2009	2008	2007
International Financial Reporting Standards (IFRS)	The Guide to the Assessment of IT Risk (GAIT)	The Guide to the Assessment of IT Risk (GAIT)	ISO 27000 (information security)	Enterprise risk management
GTAG 13 – Fraud Prevention and Detection				Fraud risk management
ISO 31000 (risk management)	International Financial Reporting Standards (IFRS)	International Financial Reporting Standards (IFRS)	Enterprise risk management	COSO Enterprise Risk Management Framework
Penalties in Administrative Proceedings (Dodd-Frank Act 929P)	Extensible Business Reporting Language (XBRL)	Extensible Business Reporting Language (XBRL)	Fraud risk management	International Financial Reporting Standards (IFRS)
				Six Sigma
Six Sigma	ISO 27000 (information security)	Enterprise risk management	COSO Enterprise Risk Management Framework	Gramm-Leach-Bliley Act (GLBA)
Hedging by Employees and Directors (Dodd-Frank Act 955)	COBIT	ISO 27000 (information security)	Fair Value Accounting (FAS 159)	U.S. GAAP
GTAG 15 – Information Security Governance				

Note that in earlier years of this study, analytics were not among the top priorities for internal auditors, but have ranked consistently at the top over the past five years.

Focus on Results by Company Size

Company Size Results, General Technical Knowledge		
Small ‹ US$1B	Medium US$1B-$9B	Large › US$10B
NIST Cybersecurity Framework	ISO 27000 (information security)	Business/digital transformation
ISO 27000 (information security)	Mobile applications	Big data/business intelligence
Big data/business intelligence	NIST Cybersecurity Framework	Cloud computing accounting standard
Business/digital transformation	GTAG 16 – Data Analysis Technologies	GTAG 16 – Data Analysis Technologies
Internet of Things	Internet of Things	Cloud computing

Focus on Chief Audit Executives

The responses from CAEs diverge in notable ways from the overall findings. Among the differences, two areas that are new to the survey, big data/business intelligence and auditing corporate culture, rank among the top five priorities for internal audit leaders.

Finding big data and business intelligence at the top of the CAE priority list is a telling sign. As organizations become increasingly data-driven, CAEs not only recognize the importance of providing clarity around the risks involved in doing so, but also understand the need for internal audit to leverage this information as part of its auditing program and activities for the organization.

The desire to improve how internal audit examines and assesses corporate culture reflects a recognition that this less tangible but increasingly important quality is drawing deeper scrutiny from regulators.

CAE Results, General Technical Knowledge		
"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Big data/business intelligence	2.7
2	ISO 31000 (risk management)	2.4
3	ISO 9000 (quality management and quality assurance)	2.6
4	GTAG 17 – Auditing IT Governance	2.5
5	Auditing corporate culture	2.9

Key Questions for CAEs

- Is the internal audit function evolving in a manner that reflects the way the organization as a whole is becoming more data-driven and more susceptible to new business risks resulting from strategies and activities related to growth and innovation?
- Is internal audit operating in a sufficiently proactive, collaborative and data-driven fashion, according to key stakeholders throughout the company and on the board of directors?
- How are internal auditors keeping abreast of regulatory, technology and marketplace changes that have the potential to affect the organization's risk profile?
- Is organizational cybersecurity addressed via a comprehensive, risk-based approach that is supported by cross-enterprise collaboration and board engagement?
- What cybersecurity reporting needs of the board of directors can internal audit help address?
- How does the audit plan address cybersecurity, IT governance, social media, cloud computing and mobile application risks?
- What investments in data analytics are needed to expand internal audit's reach and heighten its efficiency?
- How does the internal audit function assess and monitor risks related to organizational culture? How can this approach be improved?
- What training and development mechanisms are in place to strengthen internal auditors' leadership and collaboration skills?

"The pace of change continues to accelerate, making it difficult for internal audit to stay on top of all of the changes. This will continue to be a challenge for us."

– Chief audit executive, midsize manufacturing company, North America

---

CAE Results, General Technical Knowledge – 10-Year Trends

Rank	2016	2015	2014	2013	2012
1	Big data/business intelligence	NIST Cybersecurity Framework	Mobile applications	Social media applications	Social media applications
2	ISO 31000 (risk management)	Mobile applications	Cloud computing NIST Cybersecurity Framework	Recently enacted IIA Standard – Functional Reporting Interpretation (Standard 1110)	Cloud computing
3	ISO 9000 (quality management and quality assurance)	GTAG 16 – Data Analysis Technologies	GTAG 16 – Data Analysis Technologies	COSO Internal Control Framework (DRAFT 2012 version)	GTAG 13 – Fraud Prevention and Detection
4	GTAG 17 – Auditing IT Governance	The Guide to the Assessment of IT Risk (GAIT)	Social media applications	Recently enacted IIA Standards – Audit Opinions and Conclusions (Standards 2010.A2 and 2410.A1)	GTAG 16 – Data Analysis Technologies
5	Auditing corporate culture	ISO 27000 (information security)	GTAG 6 – Managing and Auditing IT Vulnerabilities	Cloud computing ISO 27000 (information security)	International Financial Reporting Standards (IFRS)

Stand-out priorities for CAEs over the past decade include ISO 27000 and GTAG 16 – Data Analysis Technologies, as well as IFRS, though its priority level has understandably diminished in recent years.

2011	2010	2009	2008	2007
International Financial Reporting Standards (IFRS)	The Guide to the Assessment of IT Risk (GAIT)	International Financial Reporting Standards (IFRS)	ISO 27000 (information security)	COSO Enterprise Risk Management Framework
GTAG 13 – Fraud Prevention and Detection	Extensible Business Reporting Language (XBRL)	The Guide to the Assessment of IT Risk (GAIT)	COSO Enterprise Risk Management Framework	Enterprise risk management
			Fraud risk management	
Penalties in Administrative Proceedings (Dodd-Frank Act 929P)	International Financial Reporting Standards (IFRS)	Extensible Business Reporting Language (XBRL)	Enterprise risk management	International Financial Reporting Standards (IFRS)
Hedging by Employees and Directors (Dodd-Frank Act 955)				
GTAG 14 – Auditing User-Developed Applications	COBIT	Enterprise risk management	Fair Value Accounting (FAS 159)	Fraud risk management
GTAG 15 – Information Security Governance				
GTAG 3 – Continuous Auditing	ISO 27000 (information security)	ISO 27000 (information security)	PCAOB Auditing Standard No. 5 (AS5)	Six Sigma
GTAG 12 – Auditing IT Projects			Gramm-Leach-Bliley Act (GLBA)	

Audit Process Knowledge

Key Findings

- Internal auditors continue to focus on improving how the function deploys technology-enabled auditing – statistical analysis tools, in particular – to gain more accurate insights concerning business risks, processes and controls.
- Several areas of IT auditing (including security, continuity, program development and new technologies) are among the top priorities, reflecting the growing business risk that cybersecurity lapses, data sharing, and other new and emerging technologies pose to organizations.
- Detecting and investigating fraud represents a key area of focus – likely another reflection of new technologies and the increasingly sophisticated ways in which fraud can occur.
- Nearly half of the top-ranked priorities over the last 10 years are tied to technology-enabled auditing and analytics.

Overall Results, Audit Process Knowledge		
"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Data analysis tools – statistical analysis	3.0
2	Auditing IT – security	3.0
3	Auditing IT – continuity	3.1
4 (tie)	Fraud – fraud detection/investigation	3.1
	Quality Assurance and Improvement Program (IIA Standard 1300) – Ongoing Reviews (IIA Standard 1311)	3.3
5	Auditing IT – program development	3.0

Commentary – Overall Findings

Respondents were asked to assess, on a scale of 1 to 5, their competency in 37 areas of audit process knowledge, with "1" being the lowest level of competency and "5" 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 29.) Figure 2 on page 28 depicts a comparison of "Need to Improve" versus "Competency" ratings in an Audit Process Knowledge landscape.

Auditing IT has never been more important to internal audit functions and to the state of the organization's overall risk profile. The rapid introduction of new technologies and the risks they present, combined with the growing frequency and magnitude of corporate cybersecurity lapses, is driving internal audit to ratchet up its IT auditing capabilities. This is clearly evident in the survey results: Four different areas of IT landed in the top 10 internal audit priorities this year (see page 29).

It is notable that auditing IT (continuity), one of the top priorities identified this year, did not crack the top 20 list of priorities in 2015. This probably reflects the new realization that cybersecurity breaches – which can threaten the daily operations of a business unit, function or an entire enterprise – are more a matter of when than if. Operating as a resilient organization requires internal auditors to help management and the IT organization ensure plans and processes are in place to maintain business continuity when a major IT disruption strikes.

Technology-enabled auditing, which includes data analysis, continuous auditing and monitoring, and the use of computer-assisted audit tools (CAATs), remains a concern. For years, our survey results have shown technology-related auditing processes and tools to be top priorities with relatively stagnant competency scores. The trend continues this year, suggesting that internal audit functions are not achieving sufficient progress in their knowledge and use of technology-enabled auditing. It's time for CAEs and internal audit professionals to reverse this trend, especially in light of the growing importance of IT auditing and the organization's increasing reliance on data analysis to drive growth and innovation.

With regard to fraud, the ability to detect fraud effectively goes hand-in-hand with data analysis capabilities, which provide a quantifiable method by which to assess and monitor fraud risk. These assets, together with technology-enabled auditing, provide the best way for internal auditors to keep their radar screens tuned at all times to potential fraud risks. Of note, a recent survey on white-collar crime and fraud risk management from Utica College and Protiviti found that relatively few companies have implemented state-of-the-art forensic data analysis.[4]

Interestingly, The IIA's Quality Assurance and Improvement Program (Standards 1300 and 1311) ranks among the top priorities this year. These standards include an external review requirement that some companies will need to complete in the coming year. The results suggest there are questions and concerns about the requirements for passing the quality assurance review (QAR). While the review is a mandatory element of the program, internal audit functions that embrace quality assurance as an ongoing priority, rather than as a checklist exercise, are better positioned to ace their external quality assessment more fluidly while boosting stakeholder confidence in the function. This said, it's important to note that it is difficult for smaller audit shops to comply with the requirements of the QAR. This could be a year when many face the requirement.

Finally, internal auditors continue to view the marketing of their function among their higher priorities. By raising awareness among the board, executive management and other leaders in the organization about internal audit's value-adding capabilities, internal audit leaders can build additional credibility that can lead to more strategic-level responsibilities.

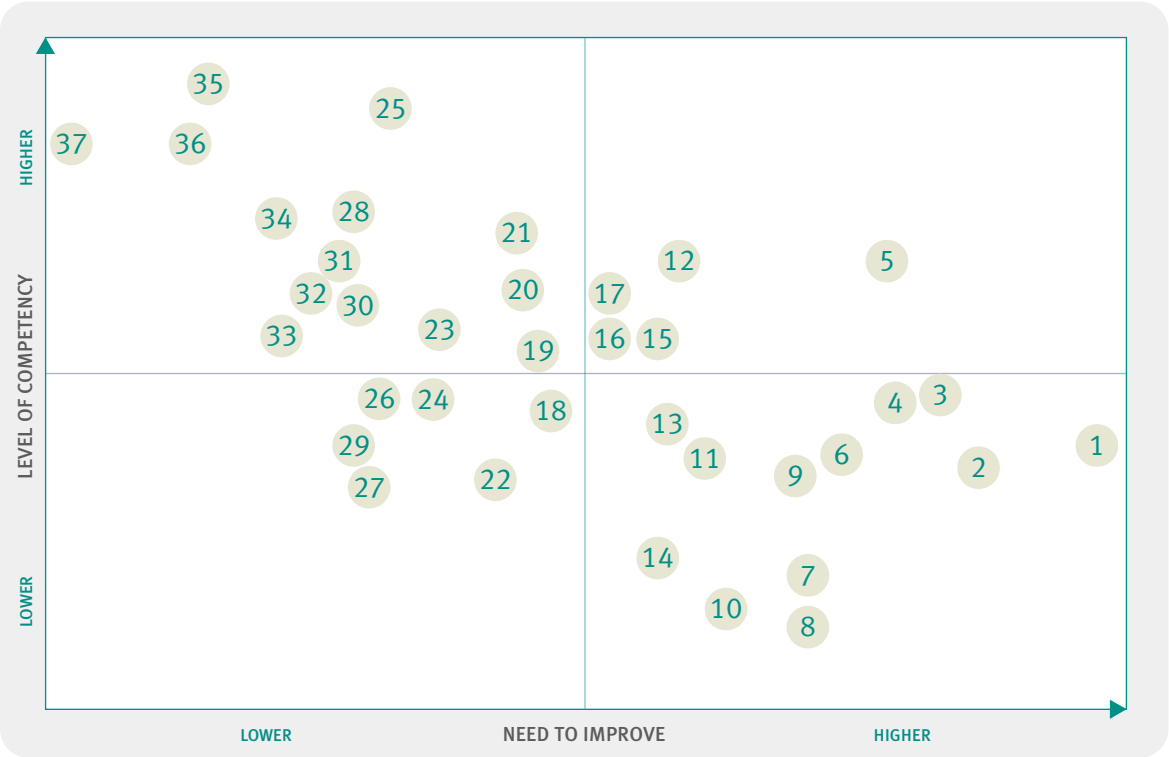
---

[4] For more information, read "Taking the Best Route to Managing Fraud and Corruption Risks," available at www.protiviti.com/fraudsurvey.

Internal Audit Action Items

- Assess the internal audit function's ability to perform all facets of IT audits, including security, continuity, program development, new technologies, computer operations, change control, and IT governance.
- Prioritize which facets of IT auditing require improvements based on organizational risk and internal audit's current capabilities, and then develop plans and investments (staff augmentation, training and development, new technology, etc.) to achieve those improvements.
- Identify and address obstacles preventing the internal audit function from more fully harnessing the benefits of technology-enabled auditing tools and approaches.
- Determine how the internal audit shop can become more data-driven.
- Assess the degree to which current expertise within internal audit supports the function's rapidly growing needs related to IT auditing and furthering technology-driven auditing; consider how to address short-term and long-term talent gaps.
- Continue to promote internal audit's capabilities throughout the organization and the board via strategic collaborations, ongoing relationship-building with all stakeholders, and ongoing demonstrations of the value of internal audit's insights and expertise.

Figure 2: Audit Process Knowledge – Perceptual Map



Number	Audit Process Knowledge	Number	Audit Process Knowledge
1	Data analysis tools – statistical analysis	20	Continuous auditing
2	Auditing IT – security	21	Operational auditing – risk-based approach
3	Auditing IT – continuity	22	Auditing IT – computer operations
4	Fraud – fraud detection/investigation	23	Assessing risk – process, location, transaction level
5	Quality Assurance and Improvement Program (IIA Standard 1300) – Ongoing Reviews (IIA Standard 1311)	24	Auditing IT – change control
6	Auditing IT – program development	25	Audit planning – process, location, transaction level
7	Assessing risk – emerging issues	26	Fraud – fraud risk assessment
8	Auditing IT – new technologies	27	Auditing IT – IT governance
9	Marketing internal audit internally	28	Operational auditing – cost effectiveness/ cost reduction
10	Computer-assisted audit tools (CAATs)	29	Quality Assurance and Improvement Program (IIA Standard 1300) – Periodic Reviews (IIA Standard 1311)
11	Continuous monitoring	30	Fraud – fraud risk
12	Data analysis tools – sampling	31	Top-down, risk-based approach to assessing internal control over financial reporting
13	Fraud – management/prevention	32	Assessing risk – entity level
14	Data analysis tools – data manipulation	33	Self-assessment techniques
15	Operational auditing – effectiveness, efficiency and economy of operations approach	34	Presenting to senior management
16	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312)	35	Audit planning – entity level
17	Fraud – monitoring	36	Report writing
18	Enterprisewide risk management	37	Audit sampling principles
19	Fraud – auditing		

Overall Results, Audit Process Knowledge – 10-Year Trends

Rank	2016	2015	2014	2013	2012
1	Data analysis tools – statistical analysis	Auditing IT – security	Computer-assisted audit tools (CAATs)	Data analysis tools – data manipulation Fraud – monitoring	Continuous auditing
2	Auditing IT – security	Computer-assisted audit tools (CAATs)	Data analysis tools – data manipulation	Auditing IT – new technologies Fraud – fraud risk assessment	Computer-assisted audit tools (CAATs)
3	Auditing IT – continuity	Data analysis tools – data manipulation	Data analysis tools – statistical analysis	Data analysis tools – statistical analysis Fraud – fraud detection/ investigation	Continuous monitoring
4	Fraud – fraud detection/ investigation Quality Assurance and Improvement Program (IIA Standard 1300) – Ongoing Reviews (IIA Standard 1311)	Marketing internal audit internally	Auditing IT – new technologies	Fraud – management/ prevention Computer-assisted audit tools (CAATs)	Data analysis tools – data manipulation
5	Auditing IT – program development	Fraud – monitoring	Data analysis tools – sampling	Data analysis tools – sampling	Data analysis tools – statistical analysis

Computer-assisted audit tools (CAATs) and data analysis tools represent the longest-running priorities over the decade we have conducted our survey. Moreover, nearly half of the top-ranked priorities over the past 10 years are tied to technology-enabled auditing and analytics. This is a clear indicator there are gaps to address.

While internal audit functions remain committed to improving how they leverage technology-enabled audit tools, a decade of results suggests progress is lacking. The question becomes why have internal audit organizations been unable to solve this puzzle. Unlike 10 years ago, there are seemingly countless data analysis and technology tools available today, and enterprise resource planning (ERP) systems can perform many of these activities with relative ease.

2011	2010	2009	2008	2007
Continuous auditing	Computer-assisted audit tools (CAATs)	Continuous auditing	Computer-assisted audit tools (CAATs)	Auditing IT – program development
		Computer-assisted audit tools (CAATs)		
Computer-assisted audit tools (CAATs)	Data analysis tools – statistical analysis	Data analysis tools – statistical analysis	Continuous auditing	Auditing IT – security
	Data analysis tools – data manipulation	Data analysis tools – data manipulation		
Data analysis tools – statistical analysis	Continuous auditing	Fraud – monitoring	Data analysis tools – data manipulation	Auditing IT – change control
Data analysis tools – data manipulation	Auditing IT – program development	Fraud – fraud detection/investigation	Data analysis tools – statistical analysis	Auditing IT – continuity
		Auditing IT – program development		
Auditing IT – program development	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312)	Fraud – auditing	Auditing IT – program development	Auditing IT – computer operations
		Fraud – fraud risk management/ prevention		
		Auditing IT – computer operations		
		Auditing IT – security		

Bottom line, despite whatever organizational or cultural resistance there may be, now is the time to embrace change and to act. Organizations that are not leveraging these technologies are likely at a tipping point where technology- and data-driven organizations will soon require an internal audit function with data analysis, continuous auditing and continuous monitoring capabilities. The trend over the past 10 years is clear. A decade from now, it is very likely that companies will not be able to afford to have an internal audit shop without these capabilities in place.

Focus on Results by Company Size

Company Size Results, Audit Process Knowledge		
Small ‹ US$1B	Medium US$1B-$9B	Large › US$10B
Assessing risk – emerging issues	Data analysis tools – statistical analysis	Data analysis tools – data manipulation
Fraud – monitoring	Auditing IT – security	Fraud – monitoring
Computer-assisted audit tools (CAATs)	Auditing IT – continuity	Auditing IT – new technologies
Quality Assurance and Improvement Program (IIA Standard 1300) – Ongoing Reviews (IIA Standard 1311)	Quality Assurance and Improvement Program (IIA Standard 1300) – Ongoing Reviews (IIA Standard 1311)	Fraud – fraud detection/ investigation
Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312)	Fraud – fraud detection/ investigation	Computer-assisted audit tools (CAATs)

Focus on Chief Audit Executives

CAE results show that internal audit leaders are placing greater emphasis on improving continuous monitoring and marketing internal audit internally. Other priorities are similar to the overall response, with auditing IT and fraud as well as The IIA's Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312) ranking among the top areas of focus for the coming year.

CAE Results, Audit Process Knowledge		
"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Continuous monitoring	3.1
2	Marketing internal audit internally	3.3
3 (tie)	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312)	3.3
	Fraud – management/prevention	3.4
4	Auditing IT – continuity	3.5
5	Auditing IT – new technologies	3.0

Key Questions for CAEs

- Is your internal audit function keeping pace with the data-driven capabilities of the rest of the organization?
- What process, people and technology changes should internal audit consider to improve its use of continuous monitoring and related technology-enabled auditing tools and approaches?
- To what degree are you and your function communicating a unified message concerning the value internal audit delivers throughout the organization and to the board?
- What specific talent plans are in place to ensure that the function can keep pace with growing demands for IT auditing?
- As internal audit's workload and priorities increase due to emerging technologies and new risks, what mechanisms are in place to ensure that less prominent but equally important priorities (e.g., fraud) receive sufficient attention?

"Fraud is only reactive. We talk about integrity as a proactive approach."

– Chief audit executive, small technology company, Europe

CAE Results, Audit Process Knowledge – 10-Year Trends

Rank	2016	2015	2014	2013	2012
1	Continuous monitoring	Auditing IT – security	Auditing IT – new technologies	Data analysis tools – data manipulation	Computer -assisted audit tools (CAATs)
2	Marketing internal audit internally	Computer-assisted audit tools (CAATs)	Computer-assisted audit tools (CAATs)	Auditing IT – new technologies	Continuous auditing
3	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312) Fraud – management/ prevention	Data analysis tools – data manipulation	Data analysis tools – data manipulation	Data analysis tools – sampling	Data analysis tools – data manipulation
4	Auditing IT – continuity	Continuous auditing	Marketing internal audit internally	Computer-assisted audit tools (CAATs) Data analysis tools – statistical analysis	Continuous monitoring
5	Auditing IT – new technologies	Data analysis tools – statistical analysis	Data analysis tools – statistical analysis	Fraud – fraud risk assessment	Data analysis tools – statistical analysis

For CAEs, data analysis tools and CAATs have ranked as priorities over most of the past decade. CAEs and other internal audit leaders should identify and address the obstacles preventing their functions from more fully leveraging technology-enabled auditing.

2011	2010	2009	2008	2007
Continuous auditing	Computer-assisted audit tools (CAATs)	Computer-assisted audit tools (CAATs)	Continuous auditing	Auditing IT – program development
		Continuous auditing		
Data analysis tools – statistical analysis	Continuous auditing	Data analysis tools – data manipulation	Data analysis tools – data manipulation	Auditing IT – security
Data analysis tools – data manipulation				
Data analysis tools – sampling	Data analysis tools – statistical analysis	Data analysis tools – statistical analysis	Computer-assisted audit tools (CAATs)	Auditing IT – computer operations
				Auditing IT – continuity
Auditing IT – computer operations	Data analysis tools – data manipulation	Fraud – monitoring	Data analysis tools – statistical analysis	Auditing IT – change control
		Fraud – fraud detection/investigation		
Fraud – monitoring	Quality Assurance and Improvement Program (IIA Standard 1300) – External Assessment (IIA Standard 1312)	Fraud – auditing	Fraud – monitoring	Marketing internal audit internally
		Fraud – fraud risk management/ prevention		

A priority that has emerged in recent years, marketing internal audit internally, reflects a sustained effort by CAEs to convey their functions' value throughout the organization.

Personal Skills and Capabilities

Key Findings

- Developing audit committee relationships represents the top internal audit personal skills priority, followed by presenting, networking and strategic thinking.
- These skills, which have ranked consistently as priorities over the past decade, are key to building more collaborative relationships with the organization and marketing internal audit internally in the most effective manner.

Overall Results, Personal Skills and Capabilities		
"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Developing audit committee relationships	3.1
2	Presenting (public speaking)	3.0
3	Developing outside contacts/networking	3.1
4 (tie)	Strategic thinking	3.5
	High-pressure meetings	3.2
5	Dealing with confrontation	3.1

Commentary – Overall Findings

Respondents were asked to assess, on a scale of 1 to 5, their competency in 19 areas of personal skills and capabilities, with "1" being the lowest level of competency and "5" 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 39.) Figure 3 on page 38 depicts a comparison of "Need to Improve" versus "Competency" ratings in a Personal Skills and Capabilities landscape.

Along with the cybersecurity and technology-related priorities discussed earlier, internal auditors are focusing more on their personal development. This is good news at a time when internal audit's success hinges on its ability to collaborate and apply its expertise at a strategic level.

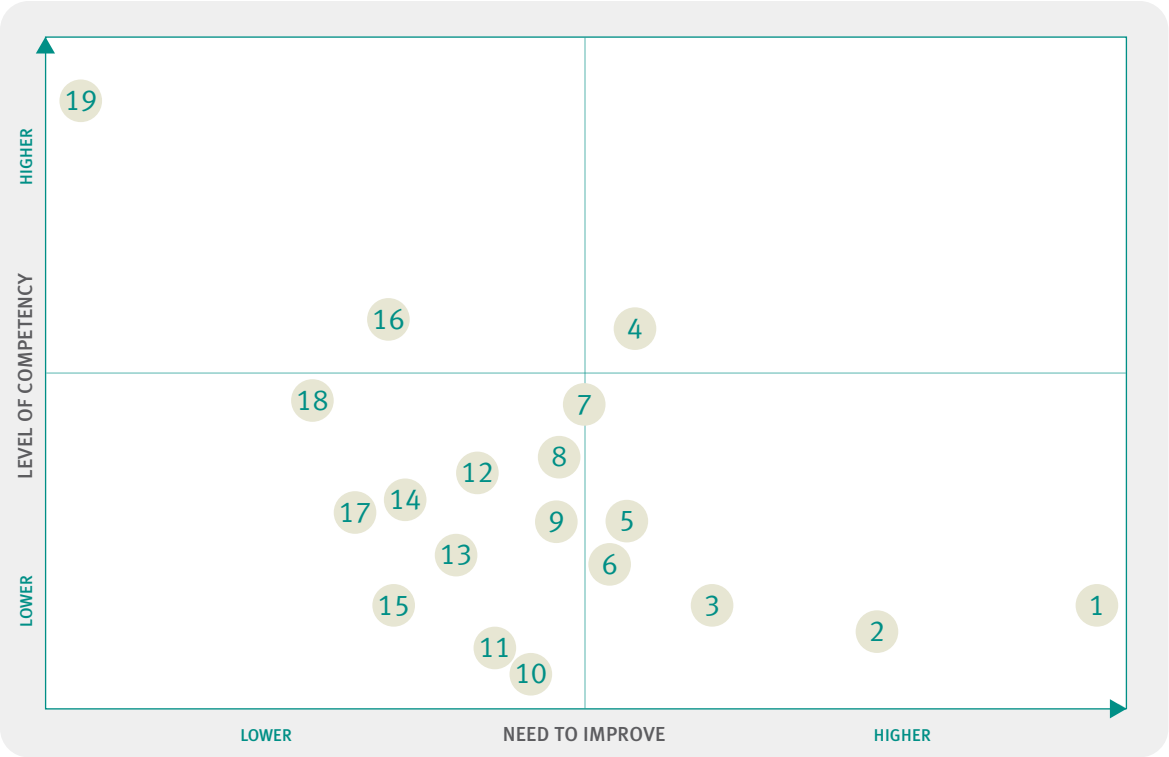
Other priorities – including the development of outside contacts/networks and deeper relationships with audit committee members – represent a broad need for internal audit to foster greater collaboration and further enhance communication channels with the board, executive management and leaders in the organization.

In addition, developing and leveraging an external personal network enables internal auditors to learn about leading practices in other organizations that may help their own functions deliver more value and/or operate with greater efficiency.

Carving out time to devote to personal skills development remains a major challenge, given the number and nature of strategic risks confronting organizations and internal audit's growing responsibilities. These are highly charged and contentious times for many companies, as evidenced by internal auditors' desire to improve how they conduct themselves in high-pressure meetings and handle confrontation. Despite these obstacles, the time to act is now to enhance these personal skills and capabilities. Internal auditors who sharpen the skills necessary to collaborate with a broad range of stakeholders will help their functions succeed in transforming into a truly strategic business partner.

Internal Audit Action Items
• Provide opportunities for more internal auditors to present to the audit committee of the board of directors in order to build rapport and credibility.
• Acknowledge the value of strategic thinking and the application of internal audit's expertise to the organization's most important business risks.
• Implement and advance training activities related to using and mastering new technology-based auditing applications and approaches.
• Encourage internal auditors to expand their professional networks, inside and outside the organization, as a way to gain access to personal development opportunities and the latest internal audit practices and thinking.

Figure 3: Personal Skills and Capabilities – Perceptual Map



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

Overall Results, Personal Skills and Capabilities – 10-Year Trends

Rank	2016	2015	2014	2013	2012
1	Developing audit committee relationships	Using/mastering new technology and applications	Presenting (public speaking)	Dealing with confrontation	Developing outside contacts/ networking
2	Presenting (public speaking)	Persuasion	Negotiation	Negotiation	Negotiation
				Persuasion	Persuasion
3	Developing outside contacts/networking	Developing other board committee relationships	Persuasion	High-pressure meetings	Dealing with confrontation
			Using/mastering new technology and applications	Presenting (public speaking)	
4	Strategic thinking	Strategic thinking	Dealing with confrontation	Strategic thinking	Presenting (public speaking)
	High-pressure meetings		Time management		
5	Dealing with confrontation	Time management	Developing other board committee relationships	Developing other board committee relationships	High-pressure meetings
			Developing outside contacts/networking	Using/mastering new technology and applications	
				Leadership (within the internal audit profession)	
				Time management	

Ten-year trends show internal audit functions that are focused on enhancing presentation and persuasion skills to build collaborative relationships with key stakeholders throughout the company and on the board.

2011	2010	2009	2008	2007
Dealing with confrontation	Presenting (public speaking)	Developing other board committee relationships	Developing other board committee relationships	Developing other board committee relationships
				Negotiation
Presenting (public speaking)	Dealing with confrontation	Dealing with confrontation	Presenting (public speaking)	Leadership (within the internal audit profession)
				Presenting (public speaking)
Negotiation	Developing outside contacts/networking	Persuasion	Developing audit committee relationships	Developing outside contacts/networking
		Presenting (public speaking)		
		Strategic thinking	Developing outside contacts/networking	
Leadership (within the internal audit profession)	Persuasion	Leadership (within the internal audit profession)	Developing rapport with senior executives	Developing audit committee relationships
		Developing outside contacts/networking	Time management	Leadership (within your organization)
		Time management		
Developing outside contacts/ networking	Strategic thinking	Developing audit committee relationships	Change management	Creating a learning internal audit function
			Creating a learning internal audit function	Persuasion
			Leadership (within the internal audit profession)	
			Negotiation	

Focus on Results by Company Size

Company Size Results, Personal Skills and Capabilities		
Small ‹ US$1B	Medium US$1B-$9B	Large › US$10B
Negotiation	Developing audit committee relationships	Presenting (public speaking)
Persuasion	Presenting (public speaking)	Developing other board committee relationships
High-pressure meetings	Developing outside contacts/ networking	Developing audit committee relationships
Time management	Strategic thinking	Persuasion
Developing outside contacts/ networking	Coaching/mentoring	Negotiation

Focus on Chief Audit Executives

The findings from CAEs are comparable to the overall response, with internal audit leaders prioritizing networking, strategic thinking and dealing with confrontation.

CAE Results, Personal Skills and Capabilities		
"Need to Improve" Rank	Areas Evaluated by Respondents	Competency (5-pt. scale)
1	Developing outside contacts/networking	3.3
2	Strategic thinking	3.5
3	Dealing with confrontation	3.2
4 (tie)	Developing audit committee relationships	3.6
	High-pressure meetings	3.4
5	Change management	3.4

Key Questions for CAEs

- Is internal audit's approach to leadership development and training sufficient, particularly as it relates to auditing IT?
- How can you give more internal audit managers face time with the audit committee as your staff strives to build rapport with audit committee members?
- What conferences, events produced by professional associations like The IIA, speaking engagements, and other external activities can strengthen your own network while giving you better access to leading risk management and internal audit thinking?
- What training and development activities related to personal skills and capabilities are included in the internal audit shop's formal talent management program?
- How can senior internal auditors mentor staff and select assignments for their direct reports in a way that helps internal auditors strengthen their strategic thinking as well as skills such as dealing with confrontation, thriving in high-pressure meetings and negotiating with stakeholders?

CAE Results, Personal Skills and Capabilities – 10-Year Trends

Rank	2016	2015	2014	2013	2012
1	Developing outside contacts/networking	Using/mastering new technology and applications	Presenting (public speaking)	Dealing with confrontation	Presenting (public speaking)
2	Strategic thinking	Developing other board committee relationships	Developing other board committee relationships	Developing other board committee relationships	Developing other board committee relationships
				Developing outside contacts/networking	Developing outside contacts/networking
3	Dealing with confrontation	Persuasion	Using/mastering new technology and applications	Negotiation	Persuasion
				Using/mastering new technology and applications	Using/mastering new technology and applications
				Time management	Negotiation
4	Developing audit committee relationships	Strategic thinking	Dealing with confrontation	Persuasion	Dealing with confrontation
	High-pressure meetings		Persuasion		
5	Change management	Leveraging others' expertise	Developing outside contacts/networking	Strategic thinking	Time management
			Negotiation		

In the past decade, CAEs have shown a sustained commitment to elevating internal audit's strategic contributions to the company by developing board committee relationships (beyond the audit committee) and by setting an example regarding the importance of improving relationship-building skills such as presenting, dealing with confrontation and strategic thinking.

2011	2010	2009	2008	2007
Developing other board committee relationships	Developing other board committee relationships	Developing other board committee relationships	Developing other board committee relationships	Leadership (within the internal audit profession)
Developing outside contacts/ networking	Presenting (public speaking)	Presenting (public speaking)	Presenting (public speaking)	Negotiation
Time management		Strategic thinking		
Leadership (within the internal audit profession)	Developing outside contacts/networking	Dealing with confrontation	Developing outside contacts/networking	Developing other board committee relationships
		Time management		Developing outside contacts/networking
Presenting (public speaking)	Time management	Developing outside contacts/networking	Time management	Presenting (public speaking)
		Negotiation	Written communication	Creating a learning internal audit function
				Leadership (within your organization)
Strategic thinking	Dealing with confrontation	Creating a learning internal audit function	Developing audit committee relationships	Persuasion
			Leadership (within the internal audit profession)	

Methodology and Demographics

More than 1,300 respondents (n = 1,333) completed questionnaires for Protiviti's Internal Audit Capabilities and Needs Survey, which was conducted in the fourth quarter of 2015.

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	13%
Audit Committee Member	1%
Director of Auditing	12%
IT Audit Director	3%
Audit Manager	24%
IT Audit Manager	4%
Audit Staff	21%
IT Audit Staff	5%
Corporate Management	3%
Management Consultant	6%
Other	8%

Size of Organization (by Gross Annual Revenue)

$20 billion or greater	10%
$10 billion - $19.99 billion	7%
$5 billion - $9.99 billion	9%
$1 billion - $4.99 billion	22%
$500 million - $999.99 million	22%
$100 million - $499.99 million	21%
Less than $100 million	9%

Industry

Financial Services (U.S.)	22%
Government/Education/Not-for-Profit	8%
Healthcare (U.S.) – Provider	8%
Healthcare (Non-U.S.)	6%
Manufacturing	6%
Real Estate	6%
CPA/Public Accounting/Consulting Firm	5%
Energy	4%
Insurance (excluding healthcare payer)	4%
Technology	4%
Retail	4%
Services	4%
Healthcare (U.S.) – Payer	3%
Distribution	2%
Financial Services (Non-U.S.)	2%
Hospitality	2%
Telecommunications	2%
Utilities	2%
Life Sciences/Biotechnology	1%
Media	1%
Other	4%

Certification

Certified Public Accountant (CPA)/Chartered Accountant (CA)	36%
Certified Internal Auditor (CIA)	31%
Certified Information Systems Auditor (CISA)	29%
Certified Fraud Examiner (CFE)	15%
Certification in Risk Management Assurance (CRMA)	10%
Certified Information Technology Professional (CITP)	9%
Certified Financial Services Auditor (CFSA)	3%
Certified Government Auditing Professional (CGAP)	2%

Type of Organization

Public	52%
Private	21%
Government	14%
Not-for-Profit	11%
Other	2%

Organization Headquarters

North America	77%
Europe	10%
Latin America	6%
Asia-Pacific	4%
Africa	1%
India	1%
Middle East	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 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. Protiviti and our independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. We also work 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.

Named one of the 2015 *Fortune* 100 Best Companies to Work For®, 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
Mark Harrison
+61.2.6113.3900
mark.harrison@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
Sanjeev Agarwal
+91.99.0332.4304
sanjeev.agarwal@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
Sydney

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*

Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

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

SAUDI ARABIA*

Riyadh

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

SOUTH AFRICA*

Johannesburg

*Protiviti Member Firm

protiviti®
Risk & Business Consulting.
Internal Audit.