Issue 5

GLOBAL PERSPECTIVES AND INSIGHTS:

Emerging Trends

Powered by Global Pulse of Internal Audit

The Institute of Internal Auditors | Global

Advisory Council

Nur Hayati Baharuddin, CIA, CCSA, CFSA, CGAP, CRMA – *IIA–Malaysia*

Lesedi Lesetedi, CIA, QIAL – *African Federation IIA*

Hans Nieuwlands, CIA, CCSA, CGAP – *IIA–Netherlands*

Karem Toufic Obeid, CIA, CCSA, CRMA – Member of *IIA–United Arab Emirates*

Carolyn Saint, CIA, CRMA, CPA – *IIA–North America*

Ana Cristina Zambrano Preciado, CIA, CCSA, CRMA – *IIA–Colombia*

Reader Feedback

Send questions or comments to **globalperspectives@theiia.org**.

Table of Contents

Methodology and Demographics

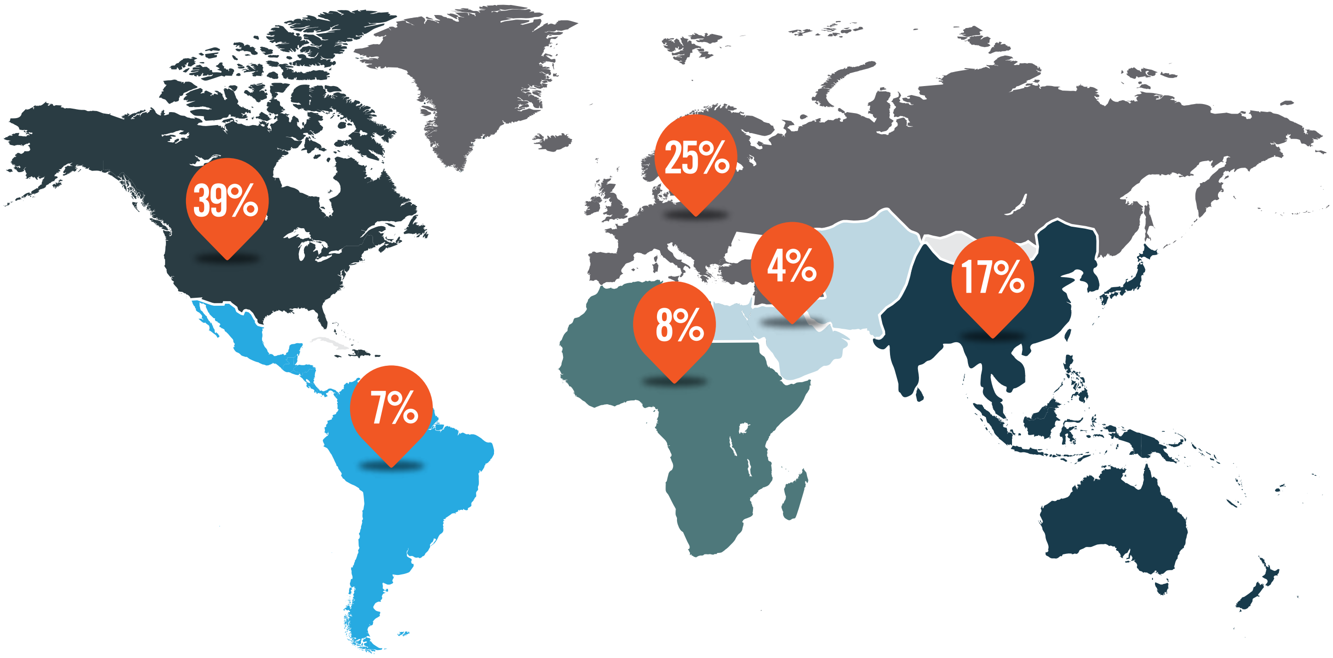
The IIA's "2016 Global Pulse of Internal Audit" survey (Global Pulse) was conducted online between 9 May and 27 May 2016.[1] The IIA collected data from 2,254 survey respondents from around the world who self-designated as current internal audit professionals. Fifty-two percent of respondents are the highest ranking member of the internal audit department, or directors/ senior managers reporting to the CAE. In this report, this group is referred to as "internal audit leaders." Respondents also include managers who report to directors (16%), audit staff who perform audits (28%), and others, including service providers (4%).

Respondents from 111 countries or territories represent a broad range of internal auditing in terms of organization type, industry, revenue, number of employees, and internal audit department size.

Respondents predominantly work in publicly traded (34%), public sector (27%), and privately held (25%) organizations.

Industries with the greatest representation include financial services (32%), manufacturing, (12%), public administration (11%), health care (6%), and utilities (6%).

Results were adjusted (normalized) to represent the global distribution of IIA members by region:



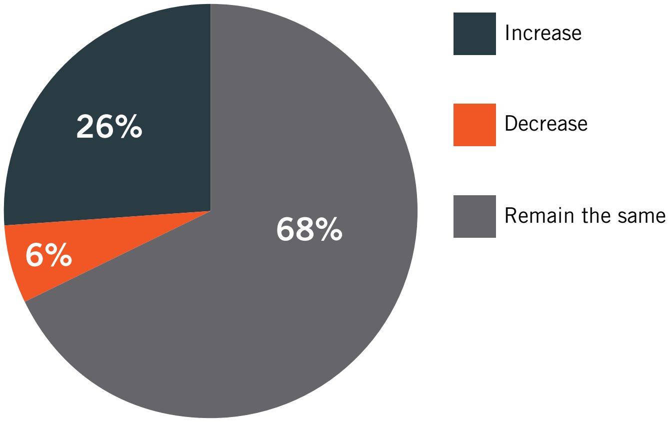
[1] For a limited number of questions, North American respondents were surveyed between 20 October 2015 and 10 November 2015.

Introduction

Across the globe, internal audit leaders are making strides toward excellence — demonstrating the business acumen, technical expertise, and relationship skills to be an invaluable resource in furthering the organization's governance, risk management, and strategic objectives. Anticipated increases in internal audit staff size and budget in many parts of the world reflect a recognition of, and support for, internal audit's elevating value by executive management and boards and enable internal audit functions to increase time devoted to critical areas such as risk management assurance, strategic business risks, and IT. But by many accounts, we need to continually get better.

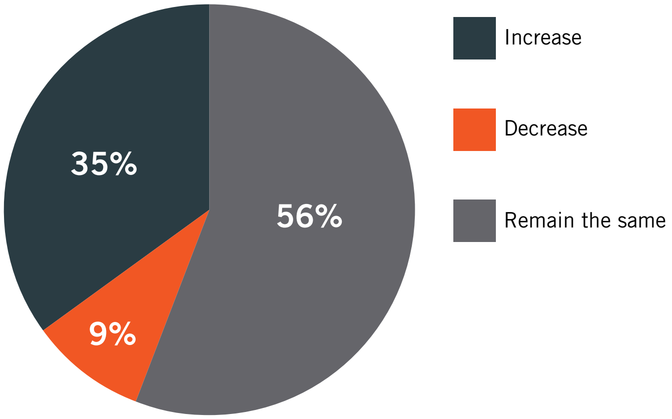
Anticipated increases in internal audit staff size and budget in many parts of the world reflect a recognition of, and support for, internal audit's elevating value by executive management and boards.

Exhibit 1 – Internal audit staffing projection



Note: Q49: Looking ahead over the next twelve months, do you expect the number of full-time equivalent staff within your internal audit function to:

Exhibit 2 – Internal audit budget projection



Note: Q50: Looking ahead over the next twelve months, do you expect the budget of your internal audit function to:

In search of steps being taken in pursuit of excellence, Global Pulse assessed the state of internal auditing by evaluating emerging issues and practices in internal audit management globally.

This report explores two emerging issues: auditing culture and keeping up with technology (cybersecurity and big data). We also explore how internal audit can, and arguably must, rise to the level of trusted adviser.

We believe that this report supports the call for internal audit to continue to focus on key emerging issues and practices. Never more so than now, the expectations being placed on internal audit continue to escalate. Yes, we have made great strides as a profession … but we also still have plenty of work to do. That is what makes internal audit such a challenging yet rewarding profession.

Auditing Culture

History shows that culture can directly and adversely affect an organization's finances, operations, and reputation. Boards, executives, and other stakeholders should be able to look to internal audit to provide assurance and advisory services that help an organization monitor and strengthen its culture, and to sound an alarm when things may be amiss.

Admittedly, internal audit has been auditing soft controls for quite some time and at least informally assessing tone at the top in many organizations since "tone at the top" became a common phrase. However, while some are taking the next step to formally audit organizational culture, the majority indicate a number of factors impeding their ability to progress.

Culture embodies an organization's beliefs and values as reflected through the actions and behaviors of all its employees. Simply said, it is the way things are done and get done throughout the organization.

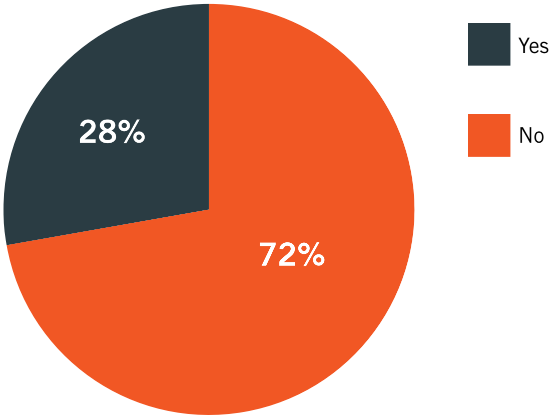
"Auditing culture is not an exact science. Many organisations struggle to define their culture, let alone incorporate it effectively into their risk evaluation and assurance processes. But it is essential that they do so."

Dr. Ian Peters, Chief Executive, Chartered Institute of Internal Auditors, (IIA–UK and Ireland)[2]

The desired culture is established at the top, appears in an organization's core values and code of ethics, and dictates acceptable and unacceptable behavior. Unacceptable, and even unethical behavior — the way NOT to do things — puts an organization at risk and, when taken to extremes, contributes to toxic organizational cultures associated with fraud, corruption, and other types of malfeasance. Some notable events have even led to economic crises and the erosion of public trust. In 2015, the world witnessed a series of high-profile incidents potentially indicative of major culture missteps, including an accounting scandal at Toshiba, allegations of bribery and corruption at FIFA, evidence of modified emissions tests at Volkswagen, and questionable reports on the impact of climate change from ExxonMobil, to name a few. Those examples alone should be a wake-up call for internal audit to provide assurance on whether or not an organization's culture is consistent with espoused core values and whether or not it encourages ethical conduct and compliance with laws and regulations. However, 72 percent of internal audit leaders indicate that they do not currently audit culture (Exhibit 3).

[2] CCH Daily, "FRC calls for greater emphasis on corporate culture," 20 Jul 2016 https://www.cchdaily.co.uk/frc-calls-greater-emphasis-corporate-culture (accessed Aug. 24, 2016).

Exhibit 3 – Percentage of internal audit departments that audit culture



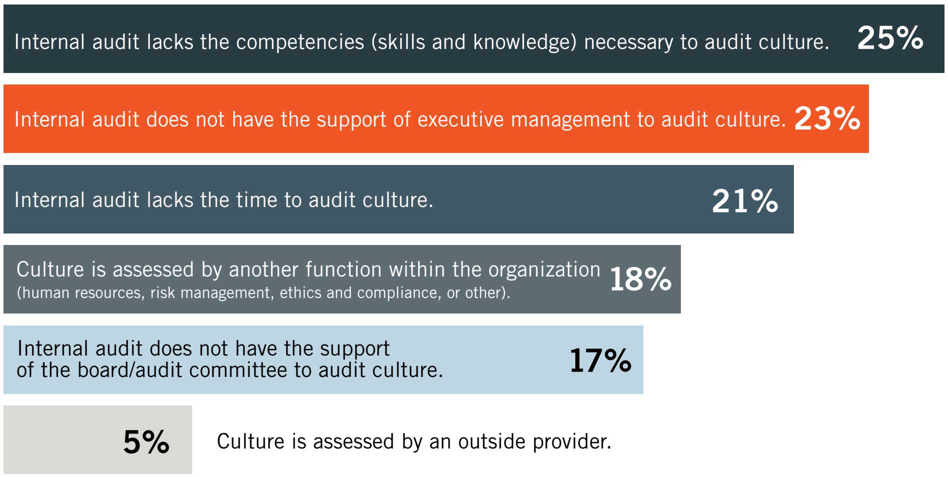
Note: Q5: Does your internal audit department audit culture?

With its comprehensive and objective view of the organization, internal audit has the potential to examine each of the microcultures, their impact on the macroculture of the organization, and the potential associated risks to the organization.

While the tone of the organization is generally set at the top and, regardless of an organization's size or complexity, a desired culture emanates from leadership, culture is not necessarily homogenous throughout the organization. A top-down, organizationwide culture — a "macroculture" — is a starting point when it comes to defining desired behavior. But every organization has many separate small cultures, or "microcultures," reflecting specific locations, departments, divisions, and other units or groups of employees with something in common. This proliferation of microcultures can make it difficult to audit culture. But with its comprehensive and objective view of the organization, internal audit has the potential to examine each of the microcultures, their impact on the macroculture of the organization, and the potential associated risks to the organization. First, internal audit must deeply understand the desired macroculture if it is then to assess subcultures and look for differences between what is desired from the top and what is actually happening across the enterprise.

Fortunately, a solid majority of internal audit leadership (89 percent) agree that their internal audit department understands the risks associated with organizational culture, but only about half (53 percent) indicate that their internal audit department actually understands *how* to audit culture. Curiously, 18 percent told us that they do not audit culture because another area performs this assessment, while top reasons for not auditing culture include a reported lack of competencies (25%) and/or not having the needed organizational support (23%) or the time (21%), as shown in Exhibit 4.

Exhibit 4 – Reasons why internal audit departments do not audit culture



Note: Q6: Which of the following describes why your internal audit department does not audit culture? Respondents could select more than one answer. (Asked of those that do not audit culture.)

> "Internal audit departments that lack skills and knowledge in auditing culture can start by doing what internal auditors do well — by bringing a systematic, disciplined approach to evaluate and improve the organization's culture-related activities."
>
> Nur Hayati Baharuddin,
> Executive Director, IIA–Malaysia

According to Nur Hayati Baharuddin, executive director of IIA–Malaysia, "Internal audit departments that lack skills and knowledge in auditing culture can start by doing what internal auditors do well — by bringing a systematic, disciplined approach to evaluate and improve the organization's culture-related activities." For example, as described in The IIA's 2016 Global Perspectives and Insights: Auditing Culture – A Hard Look at the Soft Stuff, "understanding the three lines of defense model (or other suitable model delineating risk and control duties/responsibilities and reporting lines)[3] is as effective in assessing culture as it is in supporting standard audit engagements. When it comes to auditing culture, the expected obligations for each line might include:

1. The first line of defense — business line management — is responsible for setting, communicating, and modeling desired values and conduct.

2. The second line is an oversight function, such as an ethics office, that develops ethics programs, monitors culture-related risks and compliance with culture-related policies and procedures, and provides advice to the first line.

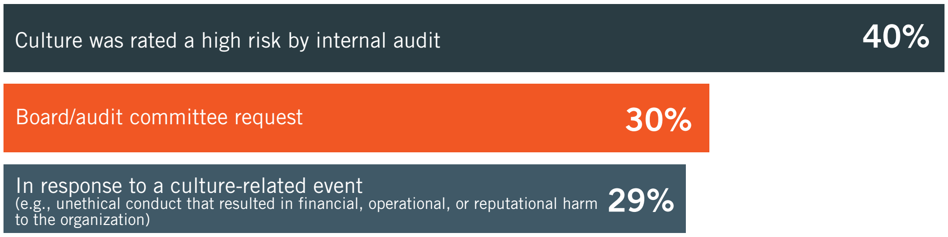
3. The third line — internal audit — evaluates adherence to the organization's stated and expected standards and evaluates whether the corporate culture supports the organization's purpose, strategy, and business model. Internal audit assesses the overall culture and identifies areas where the culture is weak."[4]

[3] The IIA's Position Paper, "The Three Lines of Defense in Effective Risk Management and Control," 2013, www.theiia.org/positionpapers (accessed Sept. 29, 2016).

[4] The IIA, "Global Perspectives and Insights: Auditing Culture – A Hard Look at the Soft Stuff," 2016, 5 www.theiia.org/gpi (accessed Aug. 24, 2016).

However, possessing the competencies or not, auditing culture *is* on internal audit's radar. According to Protiviti's 2016 Internal Audit Capabilities Survey, auditing culture ranks among the top five priorities for internal audit leaders. And remember that 89 percent of audit leadership responding to The IIA's Global Pulse survey indicate that they understand the risks associated with culture. Key motivations for auditing culture include culture being rated a high risk by internal audit, a board/audit committee request, and in response to a culture-related event (Exhibit 5).

Exhibit 5 – Why internal audit departments audit culture (top three)



Note: Q7: Please indicate why your internal audit department has audited culture. Respondents could select more than one answer. (Asked of those that do audit culture.)

Acting on this, through their leadership in developing a risk-based internal audit plan, and their relationships with the board/audit committee, CAEs must play a key role in helping their organizations maintain the healthy and desired cultures necessary for the organization to achieve its strategic mission and implement related business and operational objectives.

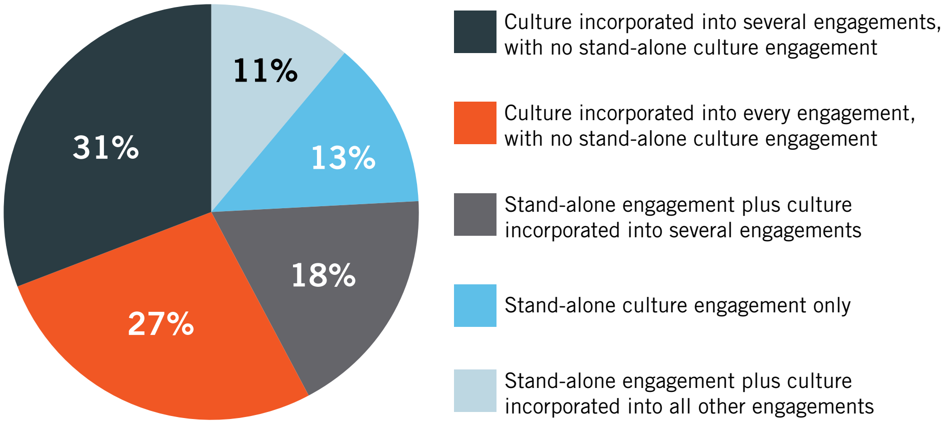
> "Auditing culture must be incorporated into every audit engagement, providing the organization with a baseline for continuous monitoring and enabling internal auditors to look for early warning signs."
>
> Angela Witzany,
> Global Chairman, The IIA

Those that do audit culture are taking a progressive approach. As expressed by The IIA's 2016–17 Global Chairman Angela Witzany, "Auditing culture must be incorporated into every audit engagement, providing the organization with a baseline for continuous monitoring and enabling internal auditors to look for early warning signs."[5]

There are at least three ways to audit culture: an organizationwide stand-alone assessment; individual engagements as part of many (if not all) audits; and/or reporting on an aggregation of a series of microculture audits conducted over time. These approaches are not mutually exclusive. Perhaps a reflection of the organization's culture itself, there are a number of different approaches cited by the minority that are auditing culture today (Exhibit 6).

[5] The IIA, "Global Perspectives and Insights: Auditing Culture – A Hard Look at the Soft Stuff," 2016, 3 www.theiia.org/gpi (accessed Aug. 24, 2016).

Exhibit 6 – Approaches to auditing culture



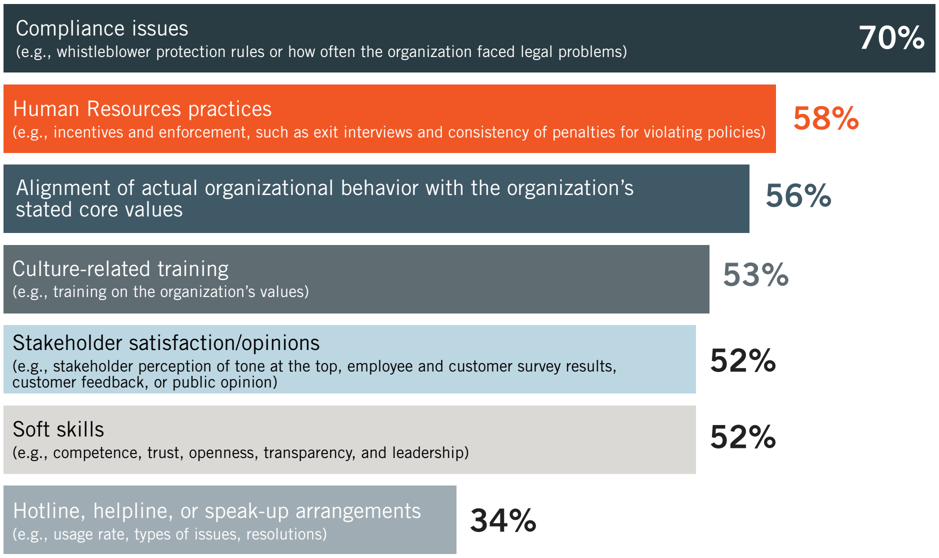
Note: Q8: Please indicate which of the following best describes your approach to auditing culture. (Asked of those that audit culture.)

At times a stand-alone culture engagement makes sense — times when a snapshot in time is necessary, such as after a major scandal, in preparation for a merger or acquisition to assess the compatibility of the organizations, or to identify the root causes for a specific noncompliance matter. However, stand-alone culture engagements are probably not sufficient on their own. When internal audit considers culture in every applicable engagement, it can better help executive management and boards detect and address a microculture that might have strayed from the desired overall organizational culture, possibly even turning toxic. So there is a place for both assessments of the macroculture, as well as the various and disparate microcultures.

Culture engagements are most effective when a comprehensive list of culture-related factors is taken into consideration — and internal audit may very well have opportunities for improvement in this area. About half of audit leaders indicate that they consider at least four out of seven factors identified in the survey (Exhibit 7). Compliance issues, human resource practices, and alignment of organizational behavior with the organization's stated core values are the factors most often considered in any culture-related engagement.

Compliance issues, human resource practices, and alignment of organizational behavior with the organization's stated core values are the factors most often considered in any culture-related engagement.

Exhibit 7 – Culture-related factors considered in internal audit engagements

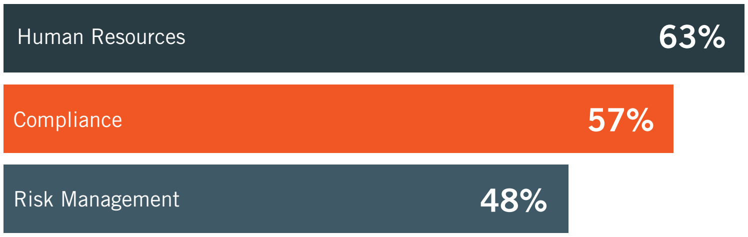


Note: Q12: Which of the following culture-related factors, if any, have been considered in any internal audit engagement? Respondents could select more than one answer. (Asked of those that audit culture.)

Interestingly, a full 60 percent of those that audit culture coordinate with other departments to do so. Most often internal audit coordinates with human resources, compliance, and/or risk management to audit culture (Exhibit 8). Coordination with other key areas in the organization appears prudent and is possibly a leading practice. However, given internal audit's important independent role, it is internal audit that should consider leading the effort and reach its own conclusions and report its opinions and observations independently.

Sixty percent of internal audit departments that audit culture coordinate with other departments to do so. However, internal audit should consider leading the effort and reach its own conclusions and report its opinions and observations independently.

Exhibit 8 – Departments that internal audit coordinates with to audit culture (top three)



Note: Q11: With which departments did internal audit coordinate with to audit culture? Respondents could select more than one answer. (Asked of those that coordinate efforts with other departments.)

We hypothesize that it may be the intangible aspects of auditing culture that explain why it may be more difficult for internal audit to report engagement results regarding culture than for other engagements. In fact, of those that are auditing culture, only about half of audit leaders report that their internal audit department understands how to report on culture, and one in five indicate that they have not reported engagement results regarding culture at all. When results are reported, the most common format is a written report, sometimes also accompanied by a verbal report.

While understandable, internal auditors should not be hesitant to tackle culture audits. When internal audit incorporates culture into every applicable engagement, culture can become one more factor to be considered in each individual set of conclusions and ultimate final report.

Conclusion

Evidence is beginning to suggest that internal audit is becoming more acutely aware of culture issues as an underlying potential cause of long-term harm to organizations. While nearly three-quarters of internal audit departments responding to this survey indicate they are not auditing culture, a smaller group of internal audit leaders have made strides toward excellence in this area. The internal audit profession at large is advised to follow these leaders by:

- Fully understanding the organization's macroculture.
- Applying established risk/governance frameworks to assess both macro- and microcultures.
- Bearing in mind multiple culture-related factors, consider culture in every engagement.
- Continuously reporting on culture.

Only about half of internal audit leaders report that their internal audit department understands how to report on culture, and one in five indicate that they have not reported engagement results regarding culture at all.

Keeping Up With Technology

While internal audit has taken some steps toward keeping up with the ever-evolving dynamics of rapidly changing and complex technology, Global Pulse survey results indicate that it appears to still struggle to comprehensively address technology risks. Internal audit is not alone in this struggle. In fact, according to the global 2016 Hewlett Packard Enterprise (HPE) report State of Security Operations, there was a year-over-year decline in security operation center (SOC) maturity in 2015. HPE attributes this decline to the pressures put on cyber defense by cloud, mobile, social, and big data computing, and the increased sophistication of the cyberattack community. Yet most any survey of board members will rate technology risks, most notably cyber, as high (if not at the very top) on the list of their concerns.

How can internal audit help? A growing number of well-informed internal audit leaders are making strides toward positioning internal audit to be an organization's trusted cyber adviser by building competencies and demonstrating proficiency in IT issues such as cybersecurity and big data, and providing a full range of internal audit services (either directly or through cosourcing) related to those issues. But for others, the Global Pulse survey data suggests that several obstacles inhibit internal audit from achieving excellence in this area.

Cybersecurity

Cybersecurity refers to the measures taken to protect company data in computer-based systems from loss, destruction, unauthorized access, or misuse by unintended parties. As explained in The IIA's 2016 Global Perspectives and Insights: Internal Audit as Trusted Cyber Adviser, "Cybersecurity must be considered holistically and systemically, as the effects of failure can range from an inability to conduct basic transactions, to loss of intellectual property, to potentially significant reputational damage. It is not solely a technology risk; it is a business risk and, as such, internal auditors have a critical role to play."[6]

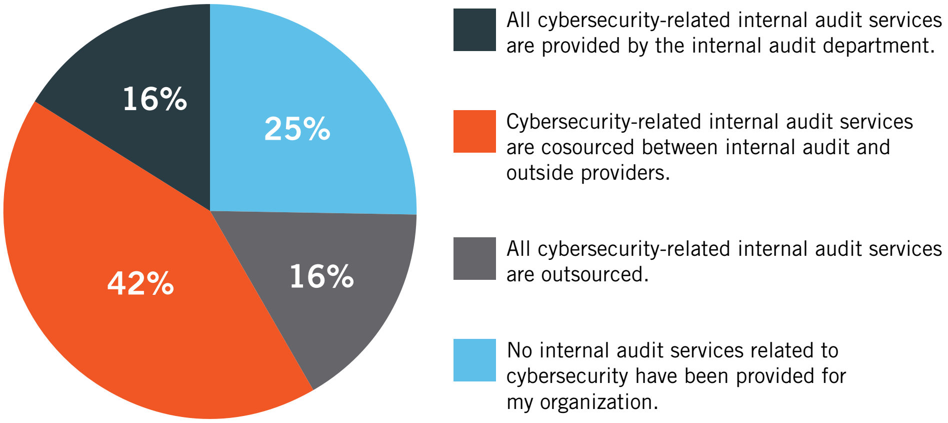
"Cybersecurity must be considered holistically and systemically, as the effects of failure can range from an inability to conduct basic transactions, to loss of intellectual property, to potentially significant reputational damage."

Fortunately, the vast majority (93 percent) of internal audit leaders report that their internal audit department understands the risks associated with cybersecurity. Contrasting that optimism, in its 2016 report, Creating trust in the digital world, EY warns that cybersecurity risks have been underestimated and that too many organizations exacerbate their vulnerabilities by taking an ad hoc approach to risk. Global Pulse confirms this, with a little more than half (55 percent) of internal audit leaders stating that their organization uses a framework designed to address cybersecurity. That is about the same number (58 percent) who say they provide cybersecurity-related internal audit services to their organization, either exclusively (16 percent) or through cosourcing (42 percent), as shown in Exhibit 9.

[6] The IIA, "Global Perspectives and Insights: Internal Audit as Trusted Cyber Adviser," 2016, 5, www.theiia.org/gpi (accessed Aug. 24, 2016).

So even though most internal audit departments may claim to understand cybersecurity risks, only a few fully translate that understanding into action by comprehensively providing all of their needed organizations' cybersecurity internal audit services. But even more alarming, given internal audit leaders' expressed understanding of cybersecurity risks and the high visibility and damage caused by well-publicized cyber events, one in four (25 percent) internal audit leaders indicate that *no* cybersecurity-related internal audit services have been provided to their organization. The remainder, 16 percent, report that all cybersecurity-related internal audit services are fully outsourced (Exhibit 9).

Exhibit 9 – Who provides cybersecurity-related internal audit services for organizations



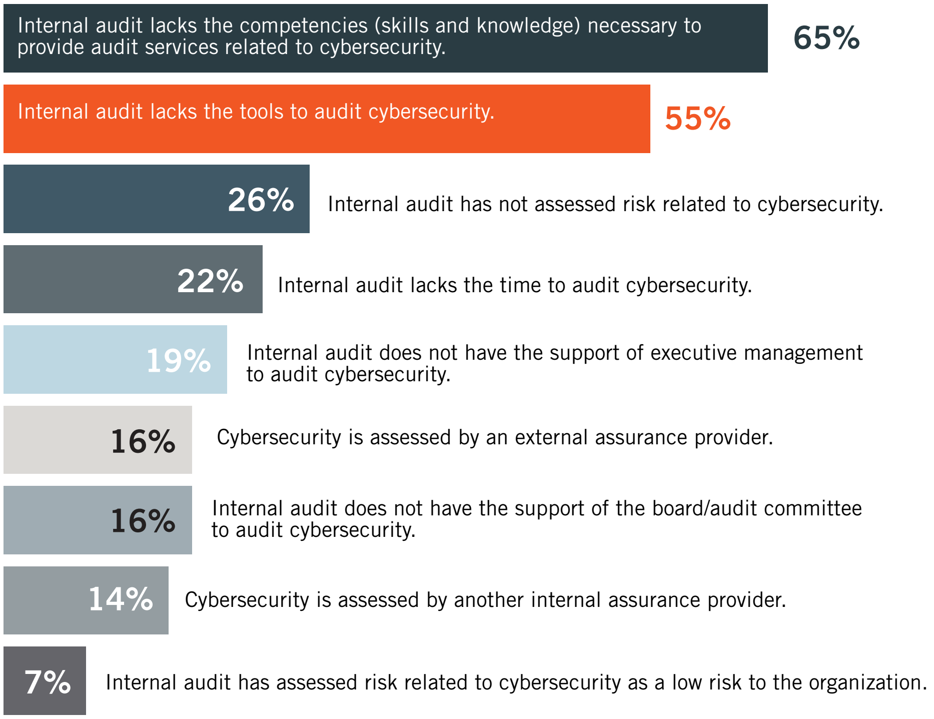
Note: Q25: Which statement best describes who provides cybersecurity-related internal audit services for your organization? Please note: Numbers do not total to 100% due to rounding.

One in four internal audit leaders indicate that no cybersecurity-related internal audit services have been provided to their organization.

The top reasons that no internal audit services were provided to the organization include that internal audit lacks the competencies (skills and knowledge) and tools to audit cybersecurity (Exhibit 10). CAEs are taking steps to correct these deficiencies. According to a 2016 IIARF CBOK report,[7] information technology and data mining/analytics are two of the seven skills that CAEs are recruiting for or building within their internal audit departments. CAEs also compensate for the lack of competencies and tools through cosourcing and outsourcing arrangements.

[7] James Rose, "The Top 7 Skills CAEs Want," (Altamonte Springs: The IIA Research Foundation, 2016) p 2, http://theiia.mkt5790.com/CBOK_2015_Top_Skills_CAEs_Want.

Exhibit 10 – Reasons why internal audit departments do not audit cybersecurity



Note: Q26: Which of the following describes why your internal audit department does not currently provide internal audit services specifically related to cybersecurity Respondents could select more than one answer. (Asked of those where no internal audit services related to cybersecurity have been provided to the organization.)

What can an internal auditor do to progress in this area? First, it all starts with having or obtaining the requisite competencies and tools to audit cybersecurity. Clearly from survey results, these are the top two impediments to successfully auditing this critical area. Then, recognize the need for support from the top. As stated in Internal Audit as Trusted Cyber Adviser, in virtually every organization, for every major project, buy-in from the top is critical. Yet boards may not be acting on their top concerns related to cybersecurity with actions commensurate with the risk. For example, according to one recent study in the United States, 26 percent of the individuals surveyed indicated that their chief information security officer (CISO) or chief security officer (CSO) makes a security presentation to the board only once a year; roughly an equal number (28 percent) reported no presentations at all. Furthermore, almost one-third said no board committees or members are engaged in cyber risk, with only 15 percent indicating engagement in cyber risk by the audit committee.[8]

[8] PwC, "US cybersecurity: Progress stalled, Key findings from the 2015 US State of Cybercrime Survey," July 2015, http://www.pwc.com/us/cybercrime (accessed Aug. 24, 2016).

Possibly as a result of some combination of both perception and reality that internal audit does not have sufficient competence in assessing cybersecurity, the confidence in internal audit picking up this shortfall is also lacking. As a case in point, in Global Pulse, only 56 percent of internal audit leaders told us that they had a mandate from the board/audit committee to audit cybersecurity. So what needs to be done? First, with its privileged access to the board/audit committee and understanding of cybersecurity risks, internal audit leaders should keep cybersecurity on the agenda, discuss cyber vulnerabilities, and offer to assist with a process for establishing the organization's cybersecurity risk appetite. For those who do not appreciate the gravity of cybersecurity risks, understand that this is a major risk factor sure to become more severe as technology continues evolving faster than the efforts to effectively risk manage and control it. In fact, Forbes reported in early 2016 a projection that cybercrime costs were expected to reach $2 trillion by 2019.[9]

With its privileged access to the board/audit committee and understanding of cybersecurity risks, internal audit leaders should keep cybersecurity on the agenda, discuss cyber vulnerabilities, and offer to assist with a process for establishing the organization's cybersecurity risk appetite.

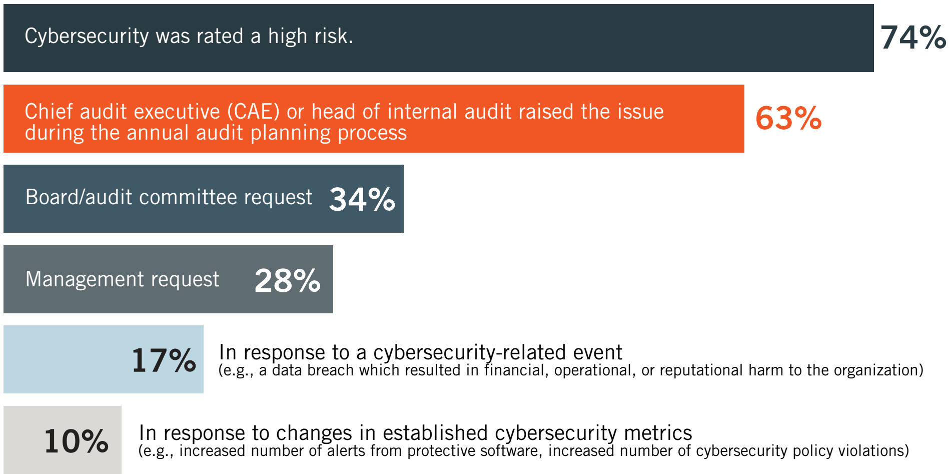
Second, realize that cybersecurity requires a collaborative effort dependent on the leadership acumen demonstrated by the CAE. As Hans Nieuwlands, chief executive for IIA–Netherlands explains, "CAEs must establish trusted partnerships with executive management, offering advice and solutions that manage or reduce cybersecurity risks to an acceptable level, and developing collaborative relationships with the chief information officer (CIO), chief information security officer (CISO), and senior privacy/legal officers."

Third, follow the lead of those who have already made strides in this area. As previously mentioned, more than half (58 percent) of internal audit leaders say they provide cybersecurity-related internal audit services to their organization, either exclusively or through cosourcing. The top reasons for auditing cybersecurity are that cybersecurity was rightfully rated a high risk, and that the CAE raised the issue during the audit planning process, demonstrating that internal audit leaders may need to be the catalyst for the organization placing the right emphasis on the ever-increasing importance of cybersecurity (Exhibit 11).

Importantly, internal audit departments that audit cybersecurity are starting to provide a wide range of valuable services to their organizations. Services cited most frequently include assessing controls that address how internet-connected systems process, store, and/or transport data, assessing the business continuity plan, and assessing the cybersecurity risk assessment process (Exhibit 12). A potentially obvious opportunity is for internal audit leaders to become more involved at the front end of the process by advising on project teams and providing guidance on cybersecurity implementation and performance plans.

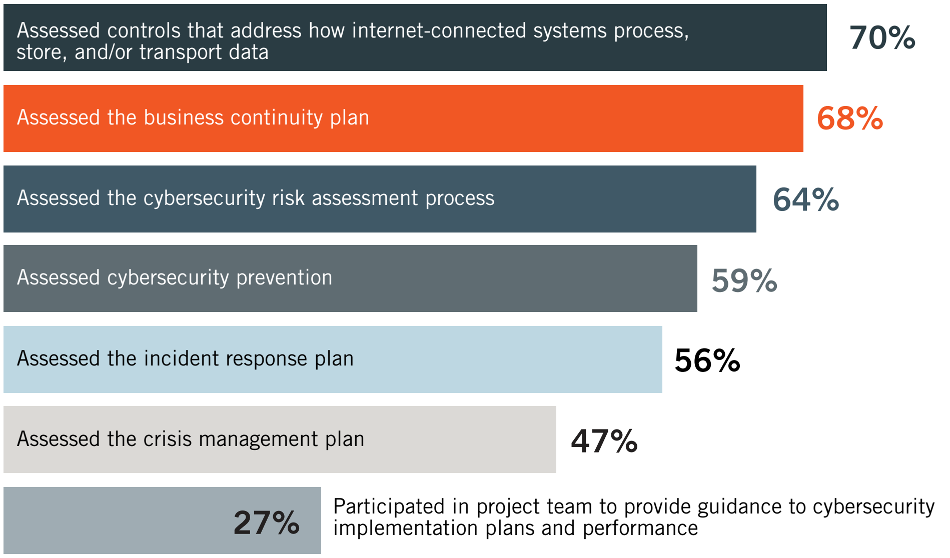
[9] Steve Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019," http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6b96d1ae3bb0

Exhibit 11 – Why internal audit departments audit cybersecurity



Note: Q27: Please indicate why your internal audit department has provided internal audit services specifically related to cybersecurity. Respondents could select more than one answer. (Asked of those that provide or cosource cybersecurity-related services.)

Exhibit 12 – How internal audit departments audit cybersecurity



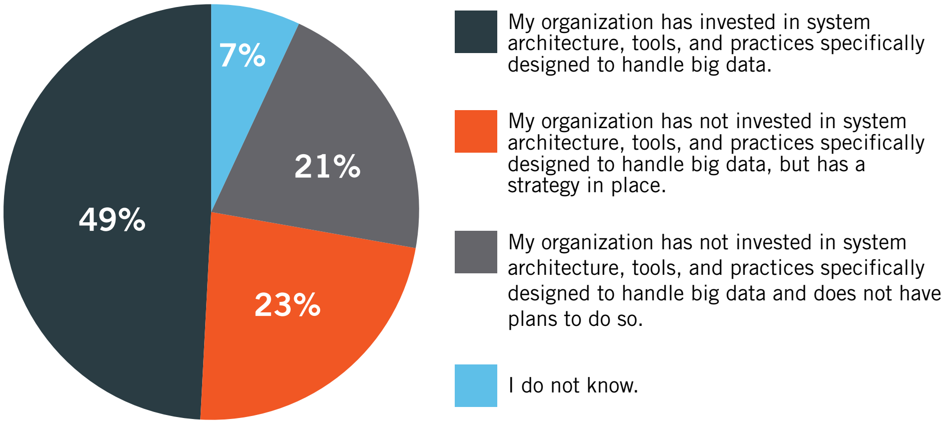
Note: Q28: Please indicate how your internal audit department has been involved with cybersecurity. Respondents could select more than one answer. (Asked of those that provide or cosource cybersecurity-related services.)

Big Data

Big data means more than just large amounts of data. Big data refers to data (information) in the organization that reaches such high volume, variety, velocity, and variability, that organizations must invest in system architectures, tools, and practices specifically designed to handle the data. Globally, nearly half (49 percent) of internal audit leaders indicate that their organizations have made such investments (and presumably have implemented systems to effectively handle big data to some degree), and another 23 percent say that their organizations have a strategy in place to do so (Exhibit 13). As a result, the expectation should be that internal audit is or will be addressing big data in its risk-based audit plans.

Globally, nearly half of internal audit leaders indicate that their organizations have made investments in big data, and another 23 percent say their organizations have a strategy in place to do so. The expectation should be that internal audit is or will be addressing big data in its risk-based audit plans.

Exhibit 13 – Organizations that have invested in big data



Note: Q17: Which statement best describes your organization's approach to big data?

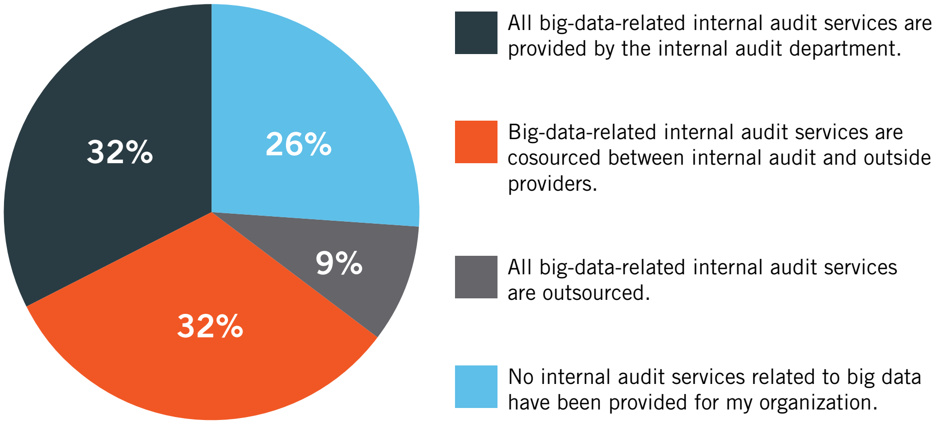
A 2016 New Vantage Partners (NVP) survey targeting senior Fortune 1000 U.S.-based business and technology decision-makers found that:

- Big data has achieved mainstream adoption.
- A new organizational role, that of chief data officer, is becoming well-established.
- Business and technology partnership is seen as critical to big data adoption.
- Business insight and speed are the main business drivers of investment in big data.
- Variety (of data) continues to outweigh volume and velocity as the technical driver behind big data investments.[10]

[10] New Vantage Partners LLC, "Big Data Executive Survey 2016," 2016, http://newvantage.com/wp-content/uploads/2016/01/Big-Data-Executive-Survey-2016-Findings-FINAL.pdf (accessed Aug. 24, 2016).

Where internal audit leaders work in organizations that have invested in big data, 64 percent say that their department provides big-data-related internal audit services to the organization, either exclusively (32 percent), or cosourced with an outside provider (32 percent), as shown in Exhibit 14. And, as with cybersecurity, internal audit leaders are oftentimes guiding the organization's attention to big data risk management and control issues. Among internal audit leaders who audit big data, the top two reasons cited for doing so are both related to seeing the risk. As reported, either the CAE raised the issue during the annual audit planning process or big data was rated a high risk by internal audit.

Exhibit 14 – Who provides big-data-related internal audit services for organizations

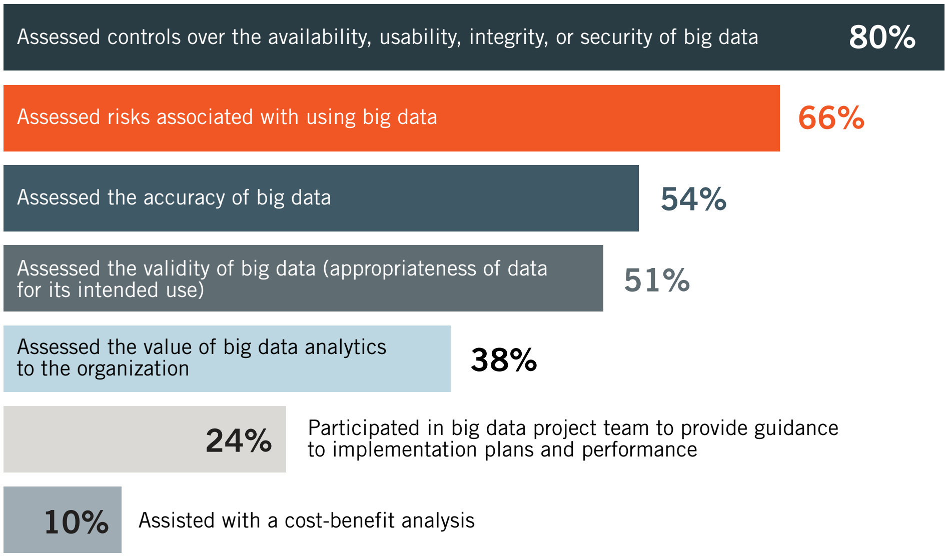


Note: Q19: Which statement best describes who provides your organization's internal audit services related to big data? (Asked of those that have invested in big data.) Please note: Numbers do not total to 100% due to rounding.

Among internal audit leaders who audit big data, the top two reasons cited for doing so are both related to risk. As reported, either the CAE raised the issue during the annual planning process or big data was rated a high risk by internal audit.

The internal audit departments that are looking at big data are providing a wide range of valuable big-data-related services to their organizations. Services cited most frequently include assessing controls over the availability, usability, integrity, or security of data; assessing risks associated with using big data; and assessing the accuracy of big data (Exhibit 15).

Exhibit 15 – How internal audit departments audit big data



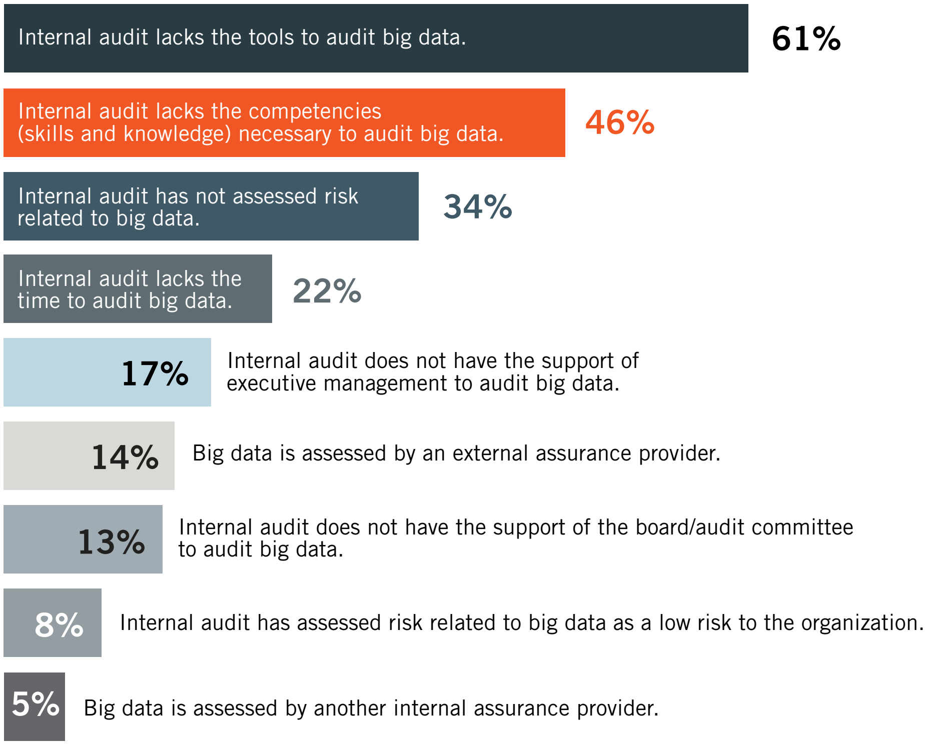
Note: Q22: Please indicate how your internal audit department has been involved with big data. Respondents could select more than one answer. (Asked of those that provide or co-source big-data-related services.)

> "When participating in project teams, internal audit can stimulate thought-provoking conversations that address both the business and technology perspectives on topics such as data integrity, security, and privacy requirements."
>
> Carolyn Saint, CAE, University of Virginia

Arguably, these internal audit services can be related to each of the key findings of the NVP survey. For example, as explained by Lesedi Lesetedi, director of internal audit at Botswana International University of Science and Technology, "The NVP survey reveals that big data spending is on the rise. Internal audit's assistance with a cost-benefit analysis can help to assure executive management and the board that the dollars spent are justified based on the potential benefits to the organization." Carolyn Saint, CAE, University of Virginia, adds that "When participating in project teams, internal audit can stimulate thought-provoking conversations that address both the business and technology perspectives on topics such as data integrity, security, and privacy requirements."

Yet despite that 92 percent of internal audit leaders report that their internal audit departments understand the risks associated with big data, and the myriad of ways that internal audit can contribute to their organization's big data initiatives, one in four (26 percent) internal audit leaders working in organizations that have invested in big data say that no internal audit services related to big data have been provided to the organization. These internal audit leaders cite a variety of reasons, though most cite a lack of tools and competencies (skills and knowledge) as being what holds internal audit back in this regard (Exhibit 16).

Exhibit 16 – Reasons why internal audit departments do not audit big data



Note: Q20: Which of the following describes why your internal audit department does not currently provide internal audit services specifically related to big data? Respondents could select more than one answer. (Asked of those where no internal audit services related to big data have been provided to the organization.)

Conclusion

Although technology risks related to cybersecurity and big data are top-of-mind for many boards, the number of internal audit departments that are providing related internal audit services to their organizations appears to not be at the level it needs to be given the risks. However, internal audit departments that do provide these services are often helping to direct the organization's attention to the critical risk and control issues associated with cybersecurity and big data. The challenge will be for internal audit to ensure it has access to the skills, knowledge, resources, and tools in an ever-changing and dynamic risk environment. Leveraging cosourcing arrangements by bringing in the appropriate subject matter expertise may prove to be imperative to many internal audit functions going forward.

Steps that will help internal audit progress toward excellence in this area include:

- Fully understanding technology-related risks and their possible impact on the achievement of operational and strategic objectives.
- Leveraging the organization's technology investments to obtain the necessary tools to audit cybersecurity and big data.
- Developing necessary internal audit competencies.
- Helping to foster cooperation between technology and business operations.
- Providing a comprehensive suite of technology-related internal audit services, from participation in project management teams to providing technology-related risk management and internal controls assurance to the board.

The number of internal audit departments that are providing cybersecurity and big-data related internal audit services to their organizations appears to not be at the level it needs to be given the risks.

Achieving Trusted Adviser Status

As elusive and challenging as it may be, internal audit has continued to make strides in keeping up with ever-elevating stakeholder expectations. For many this will be an enduring challenge, while for others it will be a matter of at least trying to stay one or two steps ahead of increasing demands and expectations.

Continuing the evolution from an arguably antiquated focus on accounting controls to true enterprisewide risk-based auditing has been a major leap forward for the profession. As well, the next maturation of the profession has been CAEs making strides to ensure an alignment of internal audit's plan with the organization's strategic priorities, and providing insights on the ability (or inability) of an organization to successfully achieve its strategic objectives.

So what's the next step? Many are now saying that internal audit needs to elevate further, being viewed across the organization as "trusted adviser" to be truly effective. Yet, in many cases, internal audit is still asking to gain the coveted "seat at the table" (if it gets one at all) — the place where the most pressing organizational issues are being discussed and executive decisions are being made. In turn, a true trusted adviser gets the seat at the table by virtue of the value everyone accepts as a given. They don't ask to be involved … they get invited. A trusted adviser, then, must have the full complement of business acumen, technical expertise, and relationship skills to be perceived by stakeholders as an invaluable resource in furthering the organization's objectives. For the CAE and their team, it means consistently having something of significant value to contribute.

A true trusted adviser gets the "seat at the table" by virtue of the value everyone accepts as a given. They don't ask to be involved ... they get invited.

In its report titled 2016 State of Internal Audit Profession Study, Leadership Matters: Advancing toward true north as stakeholders expect more, PwC revealed a gap, consistent with prevailing views, between the profession's aspirations and what it is actually delivering today. Acknowledging the expectation, only 16 percent of PwC respondents (CAEs and their stakeholders) said that internal audit today is providing value-added services and proactive strategic advice for the business well beyond the effective and efficient execution of the audit plan, while 62 percent expect internal audit to do so in the next five years. Similarly, Deloitte reported in its 2016 Global Chief Executive Survey, Evolution or irrelevance? Internal Audit at a crossroads, that "Only 28 percent of CAEs believe that their functions have strong impact and influence with the organization. A disturbing 16 percent noted that Internal Audit has little to no impact and influence. Meanwhile, almost two-thirds believe that Internal Audit's strength in these areas will be important in the coming years."[11]

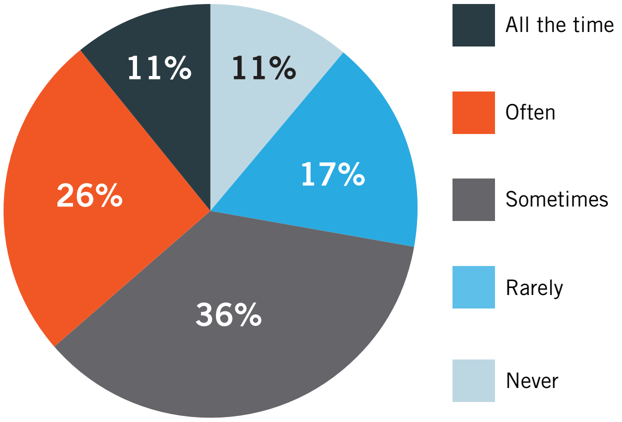
[11] Deloitte, "Evolution or irrelevance? Internal audit at a crossroads," 2016, 5, http://www2.deloitte.com/global/en/pages/audit/solutions/global-chief-audit-executive-survey.html (accessed Aug. 24, 2016).

Can internal audit close these notable gaps and make strides toward being a trusted adviser? Given the expectations, proactive and aggressive steps may need to be taken.

According to Karem Toufic Obeid, CAE, Tawazun, "Closing the gap requires building trusted relationships with executive management and the board. Trust is built when internal audit's work is not just reliable and it not only delivers on its promises, but is anticipatory and insightful." Unfortunately, the majority of internal audit leaders still meet with the CEO, executive management, and the audit committee chair only at predetermined, designated times rather than as needed and often. And building on the necessity for strong relationships at the top, having to factor in razor-sharp business acumen and technical expertise, combined with the need to be insightful, can be a tall order. But it appears that this is also becoming a necessary given. However, the majority (66 percent) of internal audit leaders report not often being asked to participate in major organizational change initiatives (Exhibit 17), and nearly one-third of internal audit leaders are *never* invited to join a full board meeting (Exhibit 18). As a result, at least at this time for many, trusted adviser status remains a hopeful "work-in-progress" aspiration.

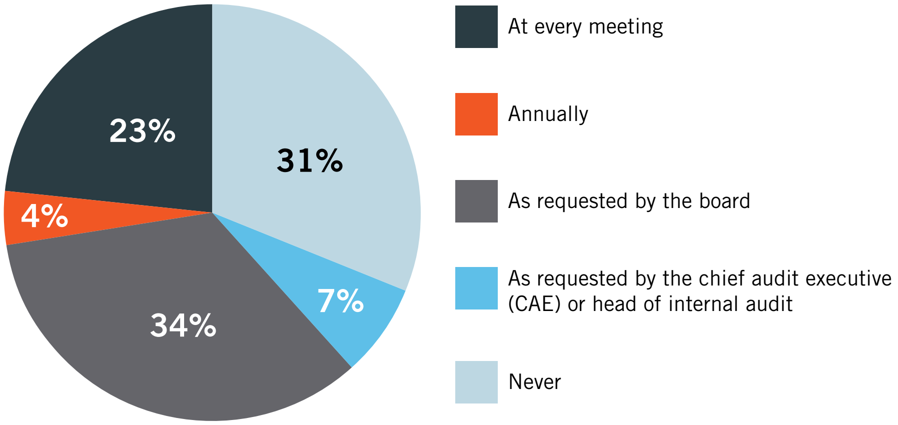
The majority (66 percent) of internal audit leaders report not often being asked to participate in major organizational change initiatives, and nearly one-third of internal audit leaders are never invited to join a full board meeting.

Exhibit 17 – How often internal audit participates in organizational change initiatives



Note: Q38: How frequently, if ever, does internal audit participate in major organizational change initiatives? Numbers do not total to 100% due to rounding.

Exhibit 18 – How often CAEs are invited to attend the full board meeting

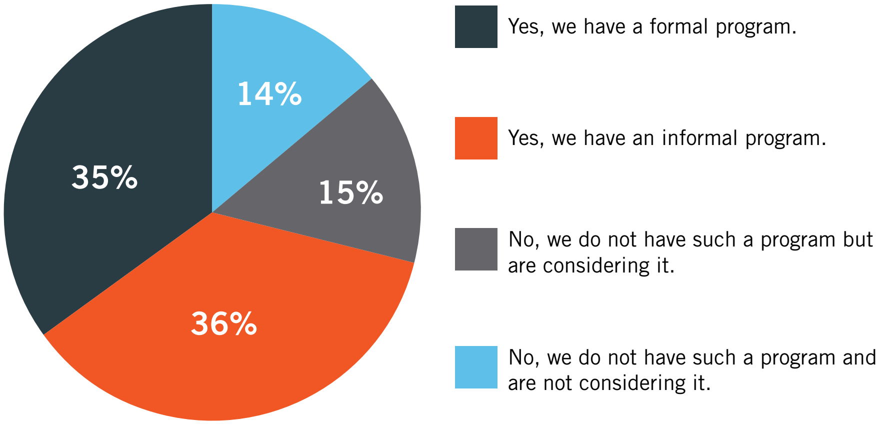


Note: Q37: How frequently, if ever, is the chief audit executive or head of internal audit invited to attend the entire board meeting (separate from the audit committee)? Numbers do not total to 100% due to rounding.

In addition to the CEO, executive management, and audit committee chair, internal audit leaders and staff need to develop relationships with senior and middle managers as well. For many, this is best accomplished through intentional planning using structured and repetitive interactions, working toward establishing deep and sustaining relationships. However, 65 percent of internal audit leaders indicate they do not have a formal program whereby internal auditors meet with targeted organizational personnel on an ongoing basis (Exhibit 19). Without such a program it will be difficult, if not impossible in most organizations of any size, for internal audit leaders and their staff to establish and sustain the baseline of relationships necessary to elevate toward being viewed as trusted advisers.

> Closing the gap requires building trusted relationships with executive management and the board. Trust is built when internal audit's work is not just reliable and it not only delivers on its promises, but is anticipatory and insightful.
>
> Karem Toufic Obeid,
> CAE, Tawazun

Exhibit 19 – Programs whereby internal auditors meet with organizational personnel

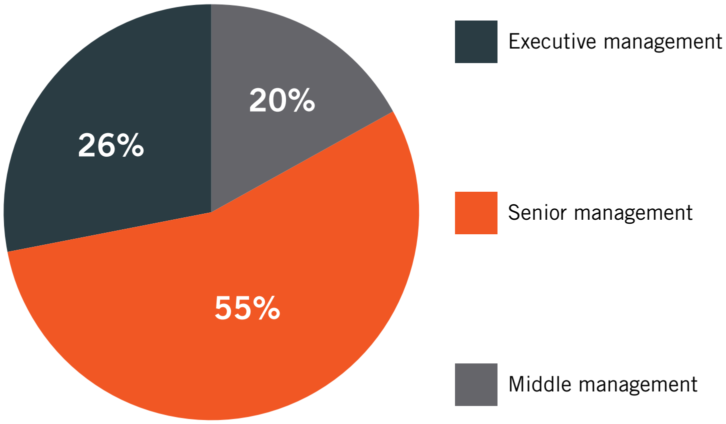


Note: Q31: Does internal audit have a program whereby internal auditors meet with organizational personnel on an ongoing basis?

Formal programs that increase internal auditor interaction with organizational personnel help internal audit become more visible, more knowledgable, and more in tune with what is truly happening within the organization. As Ana Cristina Zambrano Preciado, president and chief executive officer, IIA–Colombia, explains, "How CAEs present themselves impacts how they are perceived in the organization." And we all know that perception drives reality. Yet survey results indicate that only 26 percent of CAEs say they believe they are perceived as a member of executive management. Clearly, the remaining 74 percent do not see themselves being perceived as a peer with the executive team (Exhibit 20). Given that so many CAEs themselves do not believe they are perceived as being among the senior-most ranks of the organization, this might be viewed as a troubling statistic and a potential barrier to achieving trusted adviser status and visibility.

Only 26% of CAEs believe they are perceived as a member of executive management.

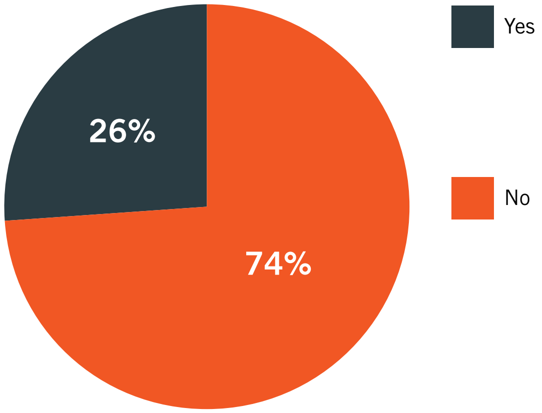
Exhibit 20 – How The CAE is perceived



Note: Q35: The chief audit executive (CAE) or head of internal audit is perceived as a member of: (Data provided reflects responses of CAEs only.) Numbers do not total to 100% due to rounding.

Another factor that may increase internal audit leaders' visibility and status in the organization, although not without challenges, is that they are being asked to take on responsibilities outside of internal audit. One in four internal audit leaders (26%) indicate that they are responsible for functions other than internal audit (Exhibit 21). Functions most often mentioned are the second line of defense-focused functions of risk management and compliance.

Exhibit 21 – Percentage of CAEs that are responsible for other functions



Note: Q39: Is the chief audit executive (CAE) or head of internal audit in your organization also responsible for any function(s) other than internal audit?

Of course, internal audit leaders face challenges when taking on responsibilities outside of internal audit. Of primary concern is maintaining both perceived and real objectivity, as well as challenges with independence depending on the reporting lines. Yes, there are risks to the blurring of the second and third lines of defense, and the CAE must strongly guard against internal audit being pulled in a direction that minimizes or compromises its primary mandate in any way. But to be asked to expand their remit beyond internal audit can also be an indicative signal to CAEs that their knowledge, skills, and contributions can be and are meaningful to the entire organization across a range of functions.

Optimal reporting lines — in the emerging view for many organizations of reporting administratively to the CEO and functionally to the audit committee — help internal audit leaders maintain organizational independence while maximizing their potential to be trusted advisers. Global Pulse reveals that 45 percent of internal audit leaders report administratively to the CEO (or equivalent), and 73 percent report functionally to the board or audit committee (or equivalent).[12] These percentages have continued to increase over time, as internal audit continues to move out from a stereotypical role of being primarily focused on only accounting and financial issues.

Being asked to expand their remit beyond internal audit — by taking responsibility for compliance or risk management for example — can be an indicative signal to CAEs that their knowledge, skills, and contributions can be and are meaningful to the entire organization across a range of functions.

[12] Administrative reporting refers to oversight of day-to-day matters, including budgeting, human resource administration, communication, internal policies, and procedures. Functional reporting refers to oversight of the responsibilities of the internal audit function, including approval of the internal audit charter, the audit plan, evaluation of the CAE, and compensation for the CAE.

Conclusion

First, from controls-based auditing to risk-based auditing, and now from bottom-up risk assessments to aligning internal audit's priorities to the strategic priorities of the organization, the next wave of evolution has arrived … that of elevating to trusted adviser status. The road ahead will require dedicated effort, as well as changing dynamics in terms of valued skills and coveted talents. But it is a road internal audit's stakeholders are beginning to expect will be traveled … and a destination a few pioneers are already achieving.

An *Internal Auditor* magazine blog from IIA President and CEO, Richard Chambers, suggested signs your contributions as CAE or internal audit may not be valued:

- Few if any audit requests come your way throughout the year.
- Minimal input is received during internal audit's annual risk assessment process.
- You are not invited to meetings where business strategy is discussed or formulated.
- Recipients of your reports are indifferent or resistant to conclusions or recommendations.
- When a significant risk is identified, management doesn't call you — they seek a consultant.[13]

[13] Chambers, Richard. June 14, 2016. Forensic Examination May Explain Why You Aren't a Trusted Advisor. https://iaonline.theiia.org/blogs/chambers/2016/Pages/Forensic-Examination-May-Explain-Why-You-Arent-a-Trusted-Advisor.aspx (accessed Aug. 24, 2016).

Closing Thoughts

With levels of budgets and staffing to support internal audit's critical activities staying the same or increasing for the majority, the opportunity for internal audit to take the extra steps necessary toward meeting and exceeding increasing stakeholder expectations may never be greater. Given the resourcing support, now may be the best time to seize the opportunity.

And, in continuing its quest for excellence and trusted adviser status, internal audit must be at the forefront to address critical organizational exposures. As the 2016 Global Pulse survey indicates, pressing exposures such as culture, cybersecurity, and big data are among the emerging issues where internal audit needs to spend, if not increase, precious time, energy, and focus.

Internal audit leaders have taken strides forward, but the profession as a whole may very well need to accelerate the pace and certainly cannot afford to lose momentum.

For More Information

Auditing Culture

- Chartered Institute of Internal Auditors, “Organizational Culture: Evolving approaches to embedding and assurance,” May 2016, https://iia.org.uk/policy/publications/culture-evolving-approaches-to-embedding-and-assurance-board-briefing/ (accessed Aug. 24, 2016).

- CCH Daily, “FRC calls for greater emphasis on corporate culture,” 20 Jul 2016 https://www.cchdaily.co.uk/frc-calls-greater-emphasis-corporate-culture (accessed Aug. 24, 2016).

- Financial Reporting Council, “Corporate Culture and the Role of Boards,” July 2016, https://www.frc.org.uk/Our-Work/Corporate-Governance-Reporting/Corporate-governance/Corporate-Culture-and-the-Role-of-Boards.aspx (accessed Aug. 25, 2016).

- The IIA, “Global Perspectives and Insights: Auditing Culture – A Hard Look at the Soft Stuff,” 2016, www.theiia.org/gpi (accessed Sept. 29, 2016).

Keeping Up With Technology

- EY, “Creating trust in the digital world,” 2015 http://www.ey.com/Publication/vwLUAssets/EY-creating-trust-in-the-digital-world/$FILE/EY-creating-trust-in-the-digital-world.pdf (accessed Aug. 24, 2016).

- KPMG, “Global profiles of the fraudster: Technology enables and weak controls fuel the fraud,” May 2016, https://home.kpmg.com/xx/en/home/insights/2016/05/global-profiles-of-the-fraudster.html (accessed Aug. 24, 2016).

- New Vantage Partners LLC, “Big Data Executive Survey 2016,” 2016, http://newvantage.com/wp-content/uploads/2016/01/Big-Data-Executive-Survey-2016-Findings-FINAL.pdf (accessed Aug. 24, 2016).

- PwC, “US cybersecurity: Progress stalled, Key findings from the 2015 US State of Cybercrime Survey,” July 2015, http://www.pwc.com/us/cybercrime (accessed Aug. 24, 2016).

- Steve Morgan, “Cyber Crime Costs Projected to Reach $2 Trillion by 2019,” http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#6b96d1ae3bb0

- The IIA, “Global Perspectives and Insights: Internal Audit as Trusted Cyber Adviser,” 2016, www.theiia.org/gpi (accessed Sept. 29, 2016).

- The IIA's Global Technology Audit Guide (GTAG), "Assessing Cybersecurity Risk: Roles of the Three Lines of Defense," 2016, www.globaliia.org/standards-guidance (accessed Sept. 29, 2016)

Trusted Adviser

- Chambers, Richard. June 14, 2016. Forensic Examination May Explain Why You Aren't a Trusted Advisor. https://iaonline.theiia.org/blogs/chambers/2016/Pages/Forensic-Examination-May-Explain-Why-You-Arent-a-Trusted-Advisor.aspx (accessed Aug. 24, 2016).

General

- Deloitte, "Evolution or irrelevance? Internal Audit at a crossroads," 2016, http://www2.deloitte.com/global/en/pages/audit/solutions/global-chief-audit-executive-survey.htm l (accessed Aug. 24, 2016).

- Protiviti, Arriving at Internal Audit's Tipping Point Amid Business Transformation, 2016, http://www.protiviti.com/en-US/Pages/IA-Capabilities-and-Needs-Survey.aspx (accessed Aug. 25, 2016).

- PwC, "2016 State of Internal Audit Profession Study, Leadership matters: Advancing toward true north as stakeholders expect more," 2016, https://www.pwc.com/ca/en/risk/publications/pwc-state-of-internal-audit-profession-study-2016-03-en.pdf (accessed Aug. 24, 2016).

- James Rose, "The Top 7 Skills CAEs Want," (Altamonte Springs: The IIA Institute of Internal Auditors Research Foundation, 2016) p 2, http://theiia.mkt5790.com/CBOK_2015_Top_Skills_CAEs_Want.

- The IIA's Position Paper, "The Three Lines of Defense in Effective Risk Management and Control," 2013, www.theiia.org/position-papers (accessed Sept. 29, 2016).

9/2016-1036

The Institute of Internal Auditors | Global

globaliia.org