2016 NORTH AMERICAN PULSE OF INTERNAL AUDIT

Time to Move Out of the Comfort Zone

The Institute of Internal Auditors

Audit Executive Center®

DISCLAIMER

ABOUT THIS DOCUMENT

The information included in this report is general in nature and is not intended to address any particular individual, internal audit function, or organization. The objective of this document is to share information and other internal audit practices, trends, and issues. However, no individual, internal audit function, or organization should act on the information provided in this document without appropriate consultation or examination. To download a digital version of this report, visit www.theiia.org/pulse.

ABOUT THE AUDIT EXECUTIVE CENTER

The IIA's Audit Executive Center® is the essential resource to empower CAEs to be more successful. The Center's suite of information, products, and services enables CAEs to respond to the unique challenges and emerging risks of the profession. For more information on the Center, visit www.theiia.org/cae.

The Institute of Internal Auditors

Audit Executive Center®

TABLE OF CONTENTS

Moving Out of the Comfort Zone 4

Auditing Organizational Culture: Relationships Matter 8

Changing the Conversation From Cybersecurity to Cyber Resiliency 16

Assessing Involvement in Organizational Use of Data 24

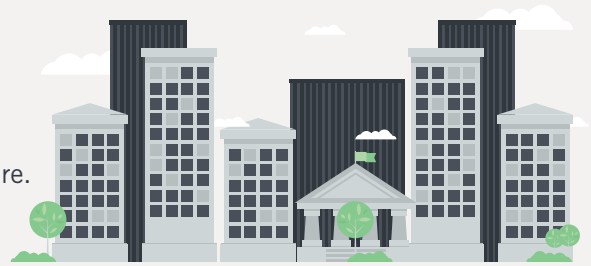
Valuing Interpersonal Skills 30

Conclusion 39

Demographics & Trending Data 41

Moving Out of the Comfort Zone

58% said they *do not* audit organizational culture.



52% reported that a lack of cybersecurity expertise among internal audit staff very much or extremely affects internal audit's ability to address cybersecurity risk.

71% reported being only moderately or less confident in strategic decisions made by the organization based on data.

65% rated their average audit team member as not at all, slightly, or only moderately proficient in accounting for the organization's politics.

58% rated their average audit team member as not at all, slightly, or moderately proficient in balancing diplomacy with assertiveness.

63% rated their average audit team member as not at all, slightly, or only moderately proficient in managing conflict effectively.

MOVING OUT OF THE COMFORT ZONE

In last year's Pulse of Internal Audit report, The IIA challenged the profession to address emerging risks by realigning audit coverage continuously — to audit "at the speed of risk." Today, the challenge remains to move beyond annual planning and typical audit areas. The consequences of a toxic culture, the destructive impact of a cyberattack, the exponential growth in the collection and reliance upon data — these represent just a sampling of today's risks that increasingly fall outside of the traditional comfort zone in which many auditors operate. As risks change, as new risks emerge, and as stakeholder expectations continue to evolve, internal auditors must move out of their comfort zone to audit at the speed of risk.

This year's IIA Pulse of Internal Audit survey focused on areas where changes in the business environment, changes in technologies, and changes in people are affecting the risk environment for organizations. How are internal auditors keeping up with these changes? In a bygone era, audit professionals carved out a comfort zone focused on financial and operational risks. The results from the survey highlight opportunities for internal audit to move out of the comfort zone.

- High-profile scandals and organizational failures that have littered the landscape over the past year point to the critical role of culture in the governance of organizations. Unfortunately, only 42 percent of survey respondents are addressing the culture in their organizations. Lack of management and board support for internal audit's involvement in culture, and lack of internal audit's ability to identify and measure organizational culture, are closely associated with internal auditors avoiding this risk.
- The issue of cybersecurity continues to present itself as a major topic of concern for organizations. Most survey respondents believe prevention is the most important response to this risk. While not ignoring the critical role of preventing cyberattacks, it has proven to be naive for many organizations to assume they can prevent a successful attack. Organizations must be prepared to respond to cyber risks, and the survey results indicate they may not be as prepared as they should be. In addition, while internal auditors recognize this risk, the majority (52 percent) acknowledge lack of expertise among internal audit as an obstacle to addressing cybersecurity risk as they should.
- Increasingly, organizations are using more data — and in more sophisticated ways — to drive decisions. Internal auditors are not as involved in all aspects of data use and only 29 percent are very or extremely confident in the strategic decisions their organizations make based on the data it collects and analyzes.

- Interpersonal skills have never been more important for internal auditors. Most CAEs are not satisfied with the level of these skills in their teams. Less than half of survey respondents reported their teams have more than a moderate level of proficiency in soft skills. The data suggests significant room for growth.

Risks keep evolving and growing and there are areas where internal audit has to move out of its traditional comfort zone and catch up to the risks. Shifts in mindset and sense of urgency are necessary for internal audit to meet and exceed the needs of their organizations — and to become trusted advisers.

Auditing Organizational Culture: Relationships Matter

WHAT ARE SOME BARRIERS TO ADDRESSING CULTURE?

24% Do not believe internal audit has freedom to assess the entire organization and staff.

35% Do not believe internal audit has full support of executive management to assess all levels of the organization.

23% Do not believe internal audit has full support of the board or audit committee to assess all levels of the organization.

Among those who DO NOT audit organizational culture

45% reported that they agree or strongly agree that internal audit is able to identify and assess measures of organizational culture.

Among those who DO audit organizational culture

80% reported that they agree or strongly agree that internal audit is able to identify and assess measures of organizational culture.

Among respondents who administratively report to the CEO

Among respondents who administratively report to the CFO

METHODS FOR ADDRESSING A TOXIC CULTURE...

21% rated focusing on organizational culture issues in audit reports as very or extremely effective.*

53% rated coordinating efforts with other governance functions as very or extremely effective.*

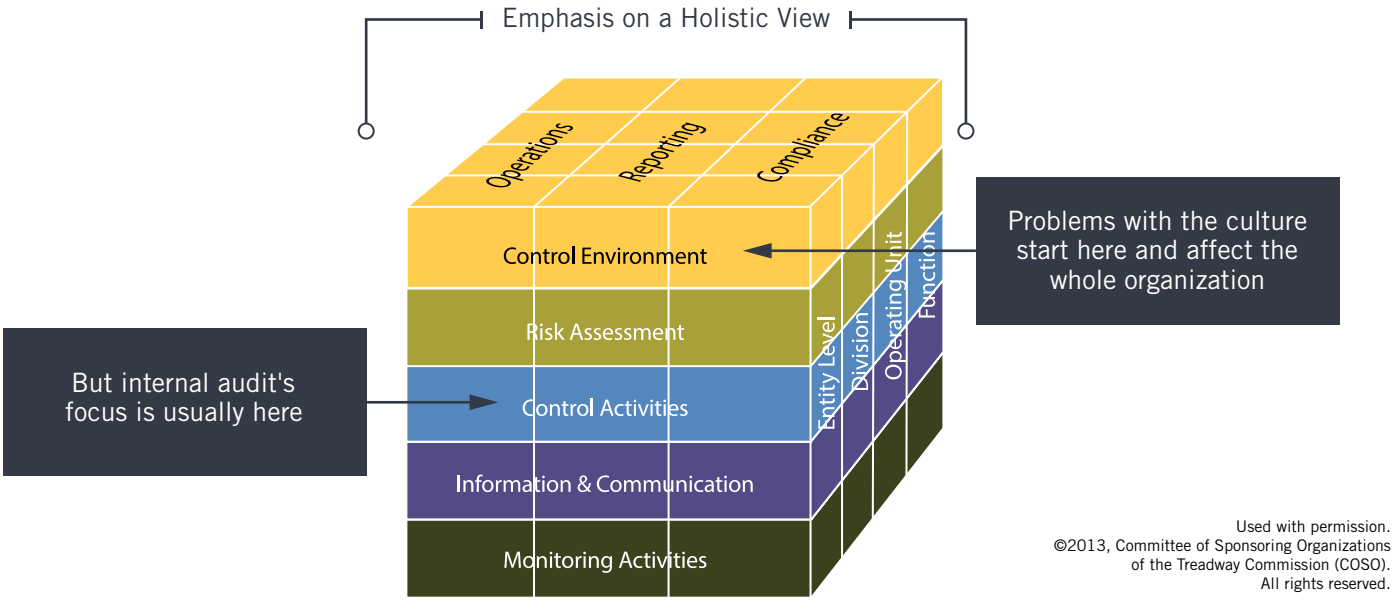
62% rated raising concerns with the board or audit committee as very or extremely effective.*

*Among respondents who audit culture.

AUDITING ORGANIZATIONAL CULTURE: RELATIONSHIPS MATTER

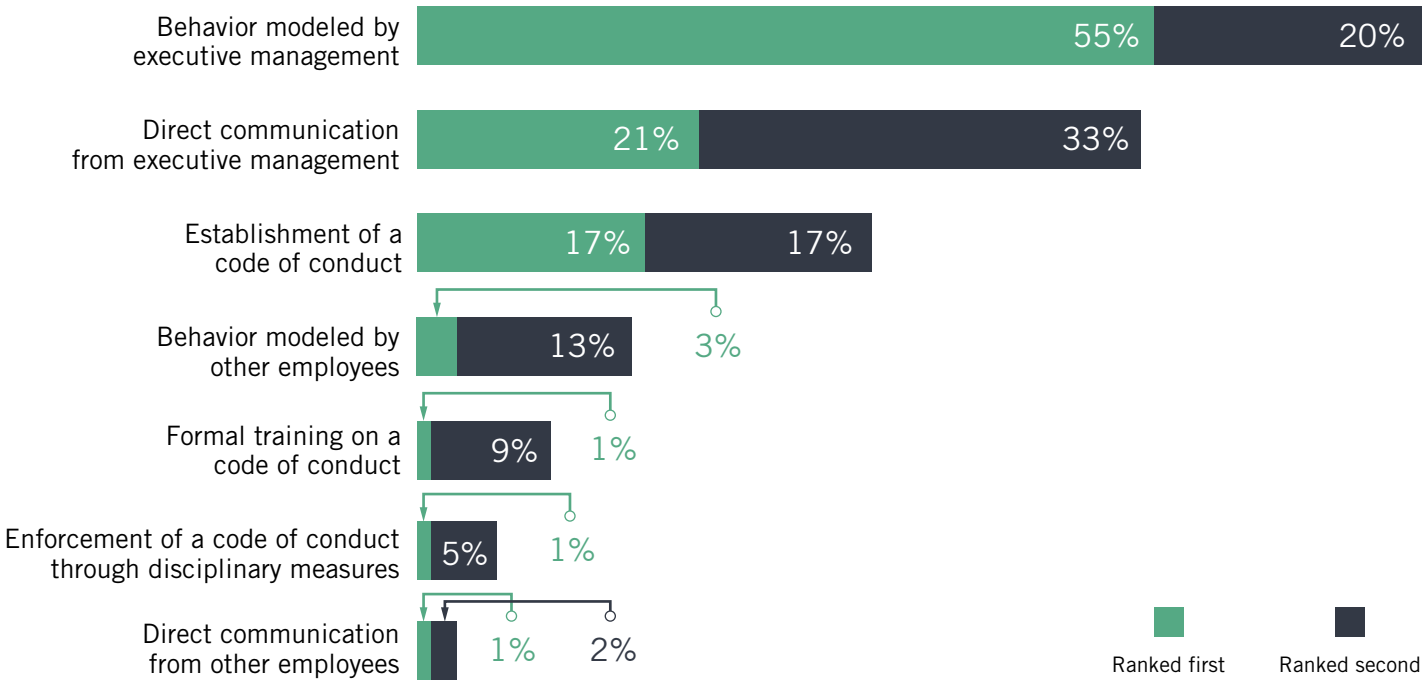
The common factor at the root of every corporate scandal from Enron to FIFA to Toshiba seems to be a culture that contributed to or condoned behavior leading to disastrous results. Culture is a key element of the control environment and organizational governance. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework emphasizes the importance of the control environment by encouraging a holistic look at organizational structure (see Figure 1).

Figure 1. COSO "Cube" Model



However, internal auditors commonly overlook culture by focusing most effort on control activities. Results from the Pulse survey indicate only 42 percent of internal auditors are addressing culture. Factors such as management integrity and ethical values as well as operating philosophy affect the control environment — probably more so than simpler objective factors. The Pulse survey asked respondents what factors were most effective in influencing culture. The top-rated factors were behavior modeled by executive management and executive management communications (see Figure 2). Considered less effective were establishment of a code of conduct and related formal training.

Figure 2. Factors influencing culture ranked as first and second most effective.

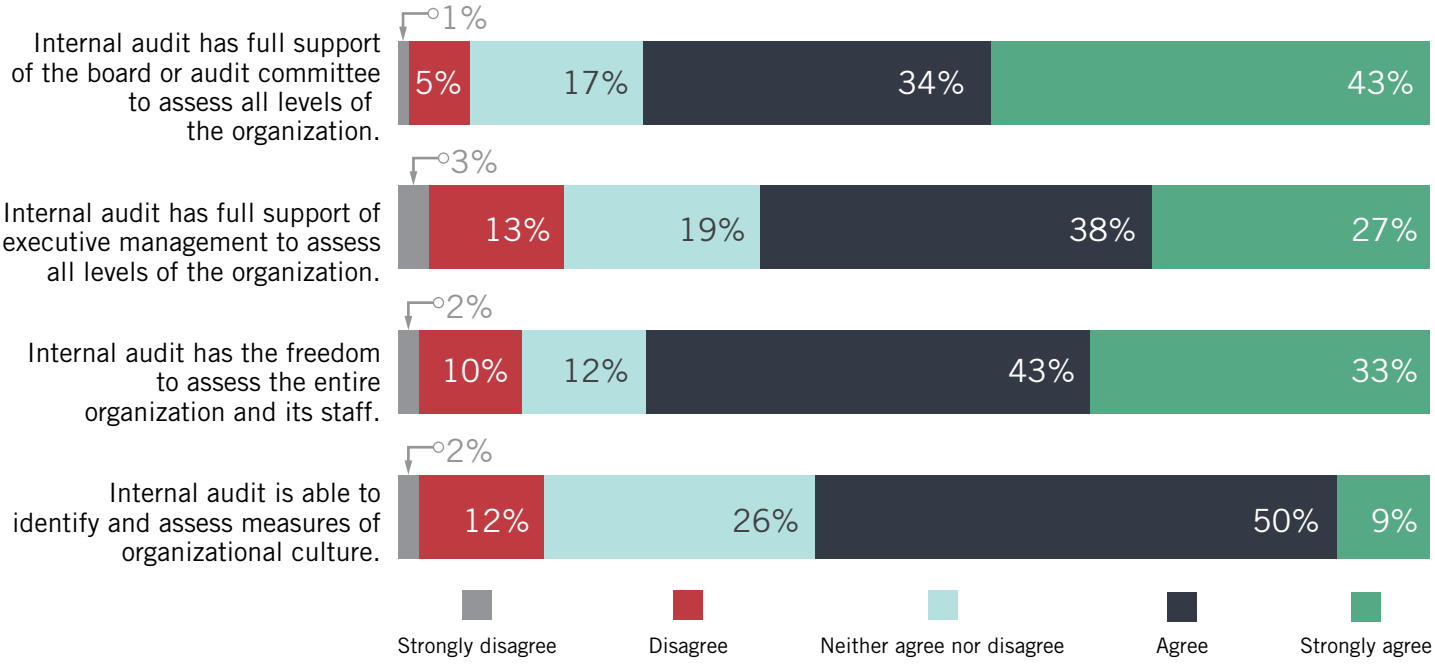


Note: Q8: Rank each of the following factors according to its effectiveness in influencing the culture of your organization, with 1 as the most effective.

In many ways culture is not an easy area to audit because assessment techniques are less defined than in more traditional audit areas. CAEs often find it is an area for which they do not have prior experience, cannot use traditional audit approaches, and may not have the full support of key stakeholders within the organization.

The majority of respondents agree or strongly agree that internal audit has the support and freedom to assess organizational culture (see Figure 3). However, there are still two concerns. First, a significant minority of respondents reported that they do not have the full support of executive management to assess all levels of the organization (35 percent) and/or do not have the full support of the board (23 percent). The internal auditors for these organizations have to fight to overcome a lack of support to address this critical aspect of governance. Second, a lack of support may be dissuading some internal auditors from auditing culture. When the Pulse survey responses are separated between those who audit culture and those who do not audit culture, it is noted that those who are not auditing culture reported substantially less support from executive management and the board for this effort.

Figure 3. Level of agreement with statements regarding internal audit's role in auditing organizational culture.



Note: Q11: Rate your level of agreement with each of the following statements regarding internal audit's role in auditing organizational culture. Totals do not equal 100 percent due to rounding.

There are others factors to consider from the Pulse survey. While most internal auditors report they have the freedom to assess the entire organization's culture (76 percent), a significant minority did not agree that they have this freedom. This may be due, in part, to the need for support from executive management and the board as respondents reported greater freedom to audit culture across the entire organization the more they had that support.

Along with the importance of organizational support, internal audit's inability to identify and assess measures of organizational culture appears to be a major obstacle to auditing organizational culture. Only 45 percent of respondents who do not audit organizational culture agreed or strongly agreed with the statement that internal audit is able to identify and assess measures of organizational culture. However, 80 percent of those who do audit organizational culture agreed or strongly agreed that they have this ability. (For comparison, see Figure 4.)

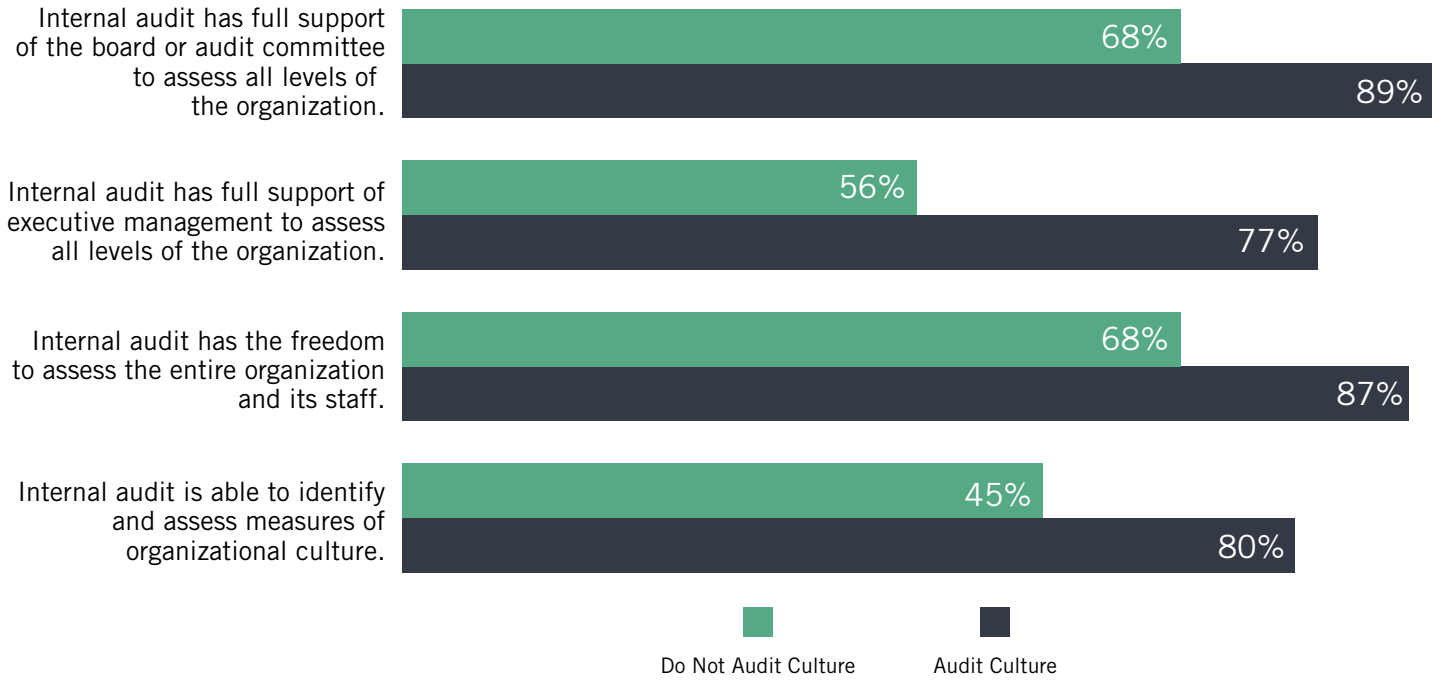
The data alone does not tell us whether the lack of organizational support and the inability to identify and assess measures of organizational culture prevent internal auditors from auditing culture. Maybe they have never sought to obtain support and ability because they have not considered auditing culture important. What is clear,

however, is culture is a key element of governance and those who audit culture have not only the requisite abilities, but also the right support from both executive management and the board.

One other interesting result from the survey is how administrative reporting lines relate to internal auditors addressing culture. The two dominant administrative reporting lines for CAEs are to the CEO and CFO. Each administrative reporting line represents 35 percent of the survey respondents. As noted earlier, only 42 percent of respondents audit culture. For those who administratively report to the CEO, the percentage who audit culture rises to 49 percent. For those who administratively report to the CFO, the percentage who audit culture falls to 33 percent. The CAE reporting line may affect whether audit focuses more on culture versus control activities and other traditional audit areas (e.g., financial audits).

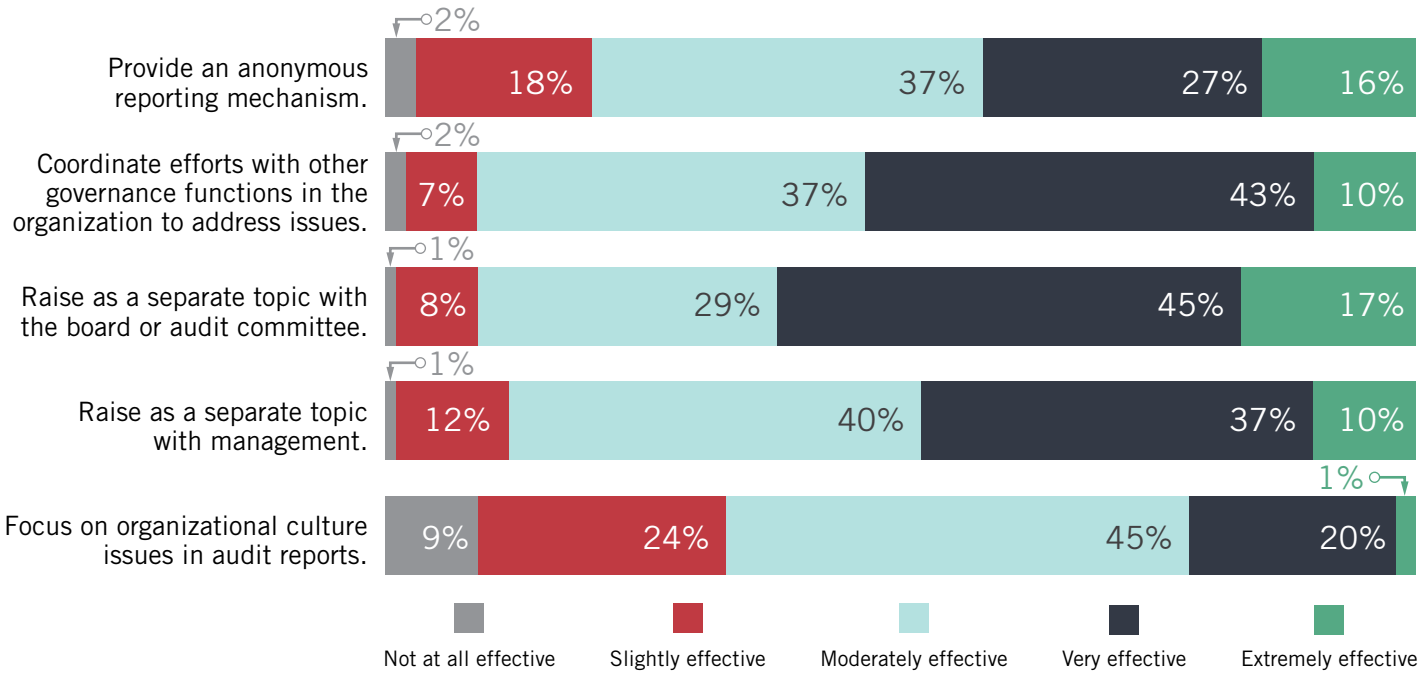
The difficulty in measuring and evaluating organizational culture presents a challenge. Whatever audit methods are used, the resulting information needs to be filtered through professional judgment and presented in a way that can

Figure 4. Comparison of respondents who do and do not audit culture. Percentage that agree or strongly agree with statements regarding internal audit's role in auditing organizational culture.



Note: Q11: Rate your level of agreement with each of the following statements regarding internal audit's role in auditing organizational culture. Answers cross-tabulated by Q6: What are your department's main driver(s) for auditing organizational culture? "Do Not Audit Culture" includes those who selected "Internal audit does not audit organizational culture." "Audit Culture" includes those who did not select "Internal audit does not audit organizational culture."

Figure 5. Effectiveness of methods addressing a toxic culture.



Note: Q12: Rate the effectiveness of the following methods for addressing a toxic culture in an organization. Includes answers from those who did not select "Internal audit does not audit organizational culture" for Q6 What are your department's main driver(s) for auditing organizational culture? *n* = 206. Totals do not equal 100 percent due to rounding.

influence change. To address issues around culture, survey respondents believe interpersonal communication is more effective than formal reports. For instance, of the respondents who do audit culture, the method most frequently identified (62 percent) as very or extremely effective for addressing issues with culture is to raise them as a separate topic with the board or audit committee. A somewhat smaller majority (53 percent) believe addressing issues with culture by coordinating efforts with other governance functions to be similarly effective. On the other hand, only 21 percent of respondents believe addressing issues with culture in audit reports is very or extremely effective. (See Figure 5.)

Both gathering and disseminating information requires that internal audit operates as a trusted adviser at all levels of relationship. From the staff auditor to the CAE, internal auditors need both relationship acumen and professional expertise to gain the confidence of peers, colleagues, executive management, and, ultimately, the audit committee and the board. For a CAE, both acumen and expertise are essential to assess culture and occupy a seat at the table, from where they have the credibility to address organizational culture and affect change. More succinctly, when it comes to addressing organizational culture, relationships matter.

IDENTIFYING HEALTHY ORGANIZATIONAL CULTURE JUST AS IMPORTANT

In a recent interview in the *Journal of Accountancy*, Jason Pett, CPA, the U.S. internal audit leader for PwC, and Peter Parillo, CPA/CFF, CGMA, vice president for internal audit for South Jersey Industries, shared the following qualities of a healthy organizational culture:

- Strong governance with clear policy and procedures.
- Communication of policy and procedures throughout the organization.
- Clear and consistent "tone at the top" communication from senior management regarding their expectations around control and appropriate behavior.
- Consistent application of policy and procedures to all levels of management without exception.
- Alignment of rewards to the right behaviors.

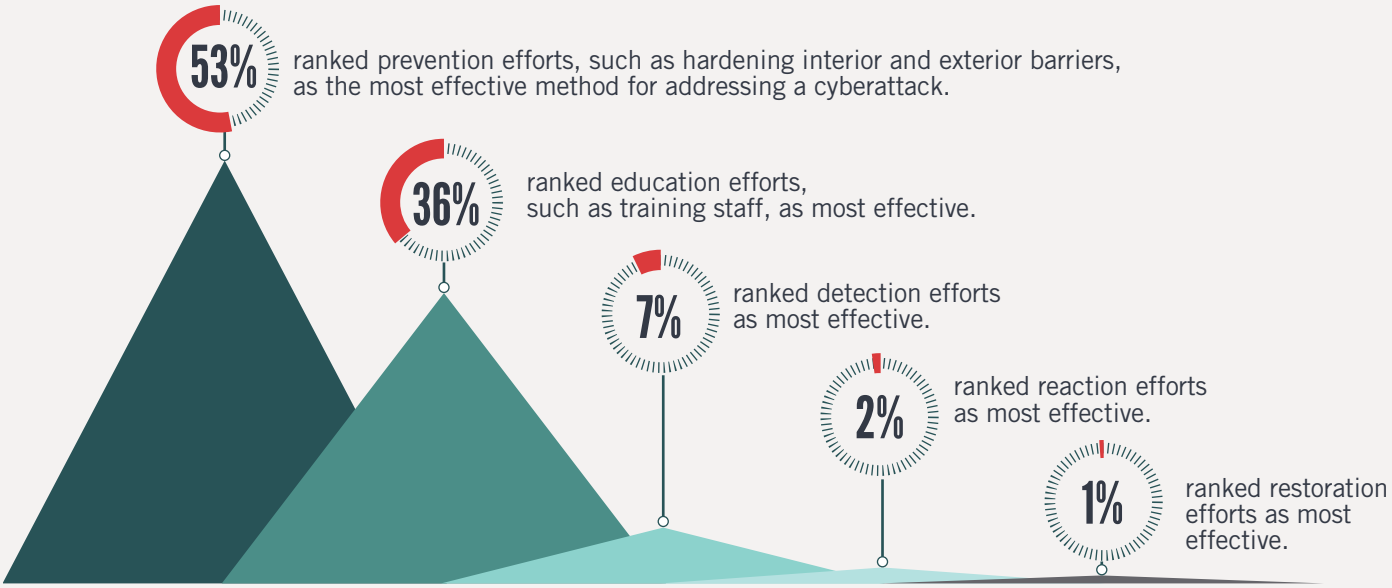
Pett noted that to address culture, internal audit needs to obtain the support of both management and the board. Additionally, Pett emphasized the importance of both understanding the business and having the respect of senior management to communicate hard messages about organizational culture.

Next Steps for the CAE

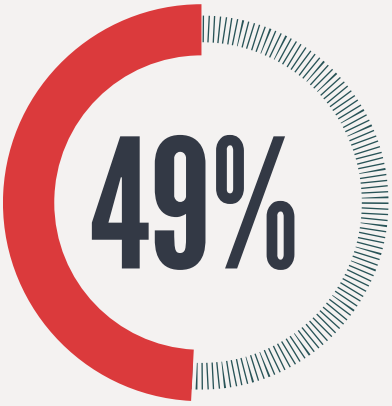
- Discuss the importance of auditing culture with the board and executive management. Make sure internal audit has the mandate it needs regarding this risk area.
- Build or acquire the skills needed to assess culture, such as understanding of the explicit and implicit motivators operating in an organization, and learning how management style affects the organization and employee behavior.
- Develop an approach to assess the critical elements of the organization's culture.
- Gather objective and subjective information about the organization's culture, using professional judgment to evaluate information that cannot be easily measured.
- Build relationships through which to identify and address concerns about culture.

Changing the Conversation From Cybersecurity to Cyber Resiliency

CYBERSECURITY PREVENTION IS FUNDAMENTAL. SHOULD CAEs SHIFT FOCUS TO CYBER RESILIENCY?



BUSINESS CONTINUITY PLANS...



Provide general procedures in response to a data breach or other type of cyberattack.

Provide clear, specific procedures in response.

Do not specify any procedures.

A GAP IN CYBERSECURITY EXPERTISE...

52% reported that a lack of cybersecurity expertise among internal audit staff very much or extremely affects internal audit's ability to address cybersecurity risk.

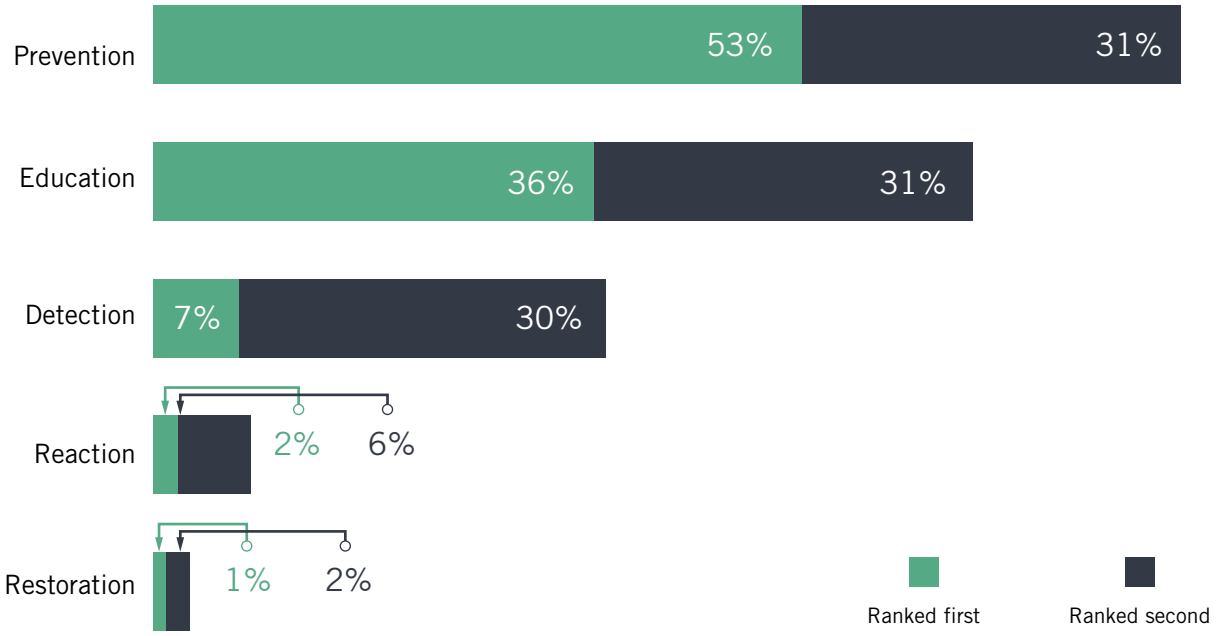
28% reported that cybersecurity and privacy skills are very or extremely essential to their internal audit function's ability to perform its responsibilities.

CHANGING THE CONVERSATION FROM CYBERSECURITY TO CYBER RESILIENCY

Cybersecurity looms large as a threat that characterizes our times. Eighty-three percent of respondents to ISACA's 2015 Global Security Status Report identified cyberattacks among the top three threats faced by organizations today. The current posture of most organizations is to focus on prevention and hence the focus of internal audit when it comes to cybersecurity is providing assurance related to preventive efforts. Respondents to the Pulse survey ranked prevention and education efforts as the most effective methods for addressing cyberattacks. Specifically, 53 percent of respondents ranked prevention efforts, such as hardening interior and exterior barriers, as most effective, and 36 percent of respondents ranked education efforts, such as training staff, as most effective. Conversely, few respondents ranked reaction and restoration efforts as the most effective method for addressing a cyberattack: 2 percent and 1 percent, respectively. (See Figure 6.)

Although preventive efforts remain a critical defense against cyberattacks, it is time to come to terms with the near inevitability of a successful breach and increase focus on all the factors that make an organization cyber resilient. Cyber resilience can be defined as the ability to resist, react to, and recover from cyberattacks — and modify

Figure 6. Methods for addressing cyberattacks ranked as first and second most effective.



Note: Q2: Rank the following methods for addressing cyberattacks in order of effectiveness, with 1 as the most effective method. Includes responses for factors ranked first and second.

PROMOTE CYBER RESILIENCY

Twenty-five percent of the respondents who reported having a business continuity plan indicated that they have detailed response procedures for a cyberattack in their plan. This means 75 percent of these respondents may not have sufficiently detailed response procedures for a cyberattack. Although a cyberattack may not be a catastrophic disruption of business activities, it remains a common risk that should be addressed in a business continuity plan.

Since cyberattacks represent a major 21st century threat, a business continuity plan without thorough response procedures for such an attack puts an organization at risk.

CAEs have the opportunity to add value to their organization by advocating for clear, specific response procedures.

an environment to increase security and sustainability[1]. While not ignoring the ability to resist an attack, an essential component of cyber resiliency is the smooth continuance of operations after a breach. Disruption of operations can have serious financial and reputational consequences.

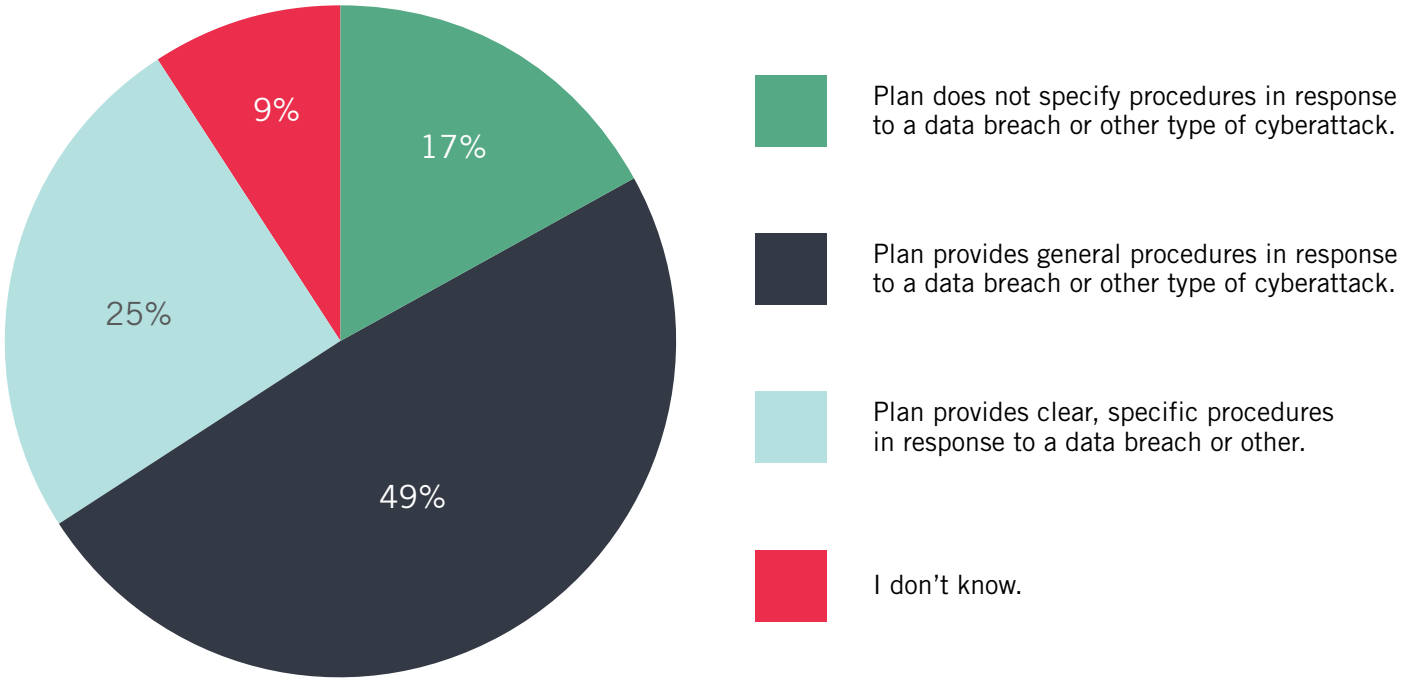
Responsive measures — such as limiting the impact of the intrusion, communicating the fact of the breach, and restoring data — should be addressed thoroughly in business continuity and disaster recovery plans or similar documents. Surprisingly, among the 95 percent of respondents who reported their organization as having a business continuity plan, only 25 percent reported that the plan provided clear, specific procedures for responding to a cyberattack — and 17 percent of respondents reported that their plans do not provide any procedures (see Figure 7). After a breach occurs, it is too late to start thinking about an appropriate response. If a business continuity plan lacks detailed response procedures for responding to a cyberattack, internal audit should ensure that the procedures are included elsewhere, such as in an incident response plan, which may or may not be linked to the business continuity plan.

Furthermore, significant gaps exist between actual and ideal levels of effort. As illustrated in Figure 8, the majority of respondents reported they believe internal audit should demonstrate significant or extremely significant effort in four areas:

- Provide assurance over readiness and response to cyberthreats.
- Communicate to executive management and the board the level of risk to the organization and efforts to address such risks.

1. *EY. "Achieving resilience in the cyber ecosystem." December 2014. http://www.ey.com/Publication/vwLUAssets/cyber_ecosystem/$FILE/EY-Insights_on_GRC_Cyber_ecosystem.pdf*

Figure 7. How would you best describe your organization's business continuity plan as it relates to cybersecurity risk?



Note: Q1.1: How would you best describe your organization's business continuity plan as it relates to cybersecurity risk? Includes respondents who indicated that their organizations have a business continuity plan. *n* = 457.

- Work collaboratively with IT and other parties to build effective defenses and responses.
- Ensure communication and coordination among all parties in the organization regarding the risk.

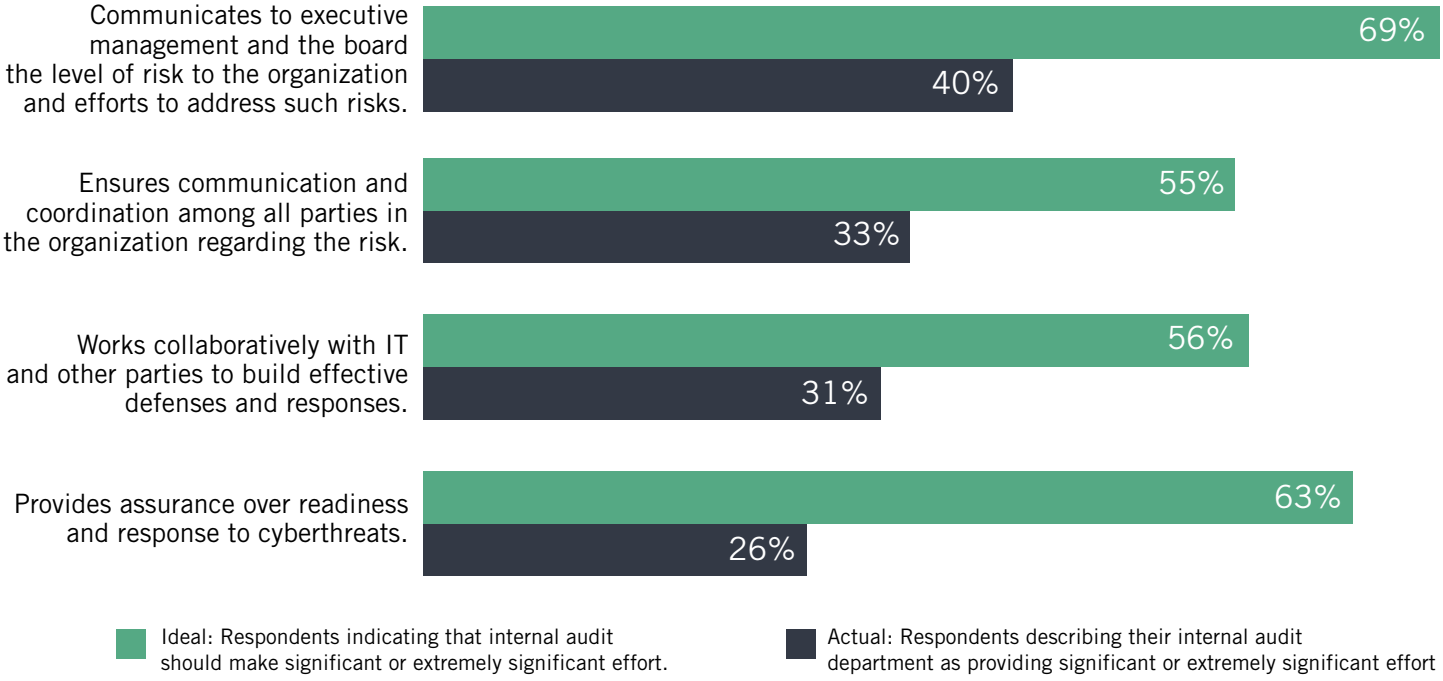
However, for none of these four areas is the internal audit skill level close to the desired level. According to the Pulse survey, several factors appear to contribute to these gaps — most significantly the lack of cybersecurity expertise in internal audit. Half of the survey respondents (52 percent) believe lack of cybersecurity expertise among internal audit staff very much or extremely affects internal audit's ability to address cybersecurity risk (see Figure 9). Yet surprisingly few respondents prioritize cybersecurity among internal audit skills. Only 28 percent consider cybersecurity and privacy skills very or extremely essential to their internal audit function's ability to perform its responsibilities. Many internal audit functions may co-source or outsource to bridge the gap for cybersecurity and privacy needs. Yet if the majority of respondents note a lack of cybersecurity expertise among internal audit staff in general, but do not perceive cybersecurity skills as essential, is internal audit naive in believing the essential ingredients are in place to address cybersecurity risk? It

may be that internal audit is uninformed about the expertise needed to address cybersecurity or that it lacks the resources to hire the necessary talent.

The potentially disastrous effects of a cybersecurity breach justify investing in the talent needed to address this major threat of the digital age. Although outsourcing and co-sourcing can provide cybersecurity talent needed for specific engagements, CAEs need to build cybersecurity knowledge within their team. CAEs should approach cybersecurity risk by applying the same principles used for other risk areas:

- Know your data.
- Conduct a risk assessment of your data controls.
- Suggest security controls to remediate weaknesses[2].

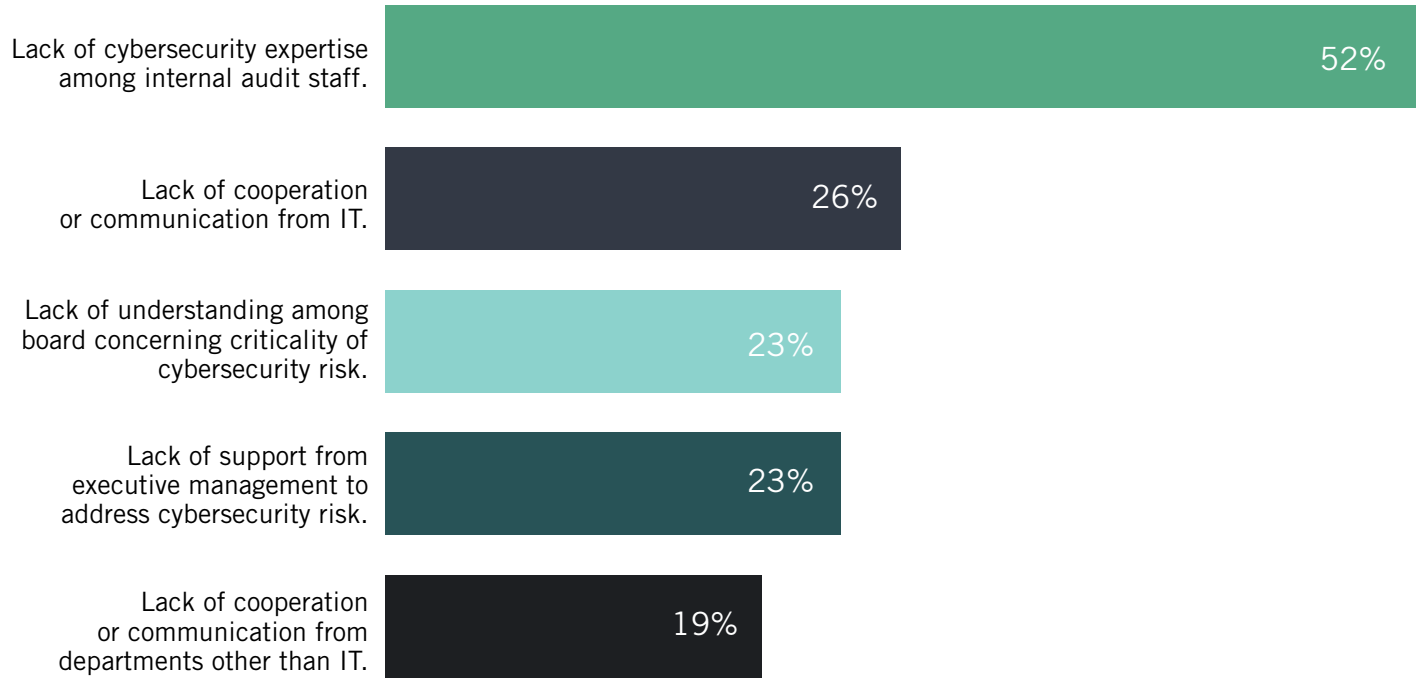
Figure 8. Comparison of ideal and actual levels of effort concerning cybersecurity.



Note: Q3: Describe the current level of effort your internal audit department is making in each of the following areas in regard to cybersecurity and Q4: Describe the level of effort an internal audit department should have in each of the following areas in regard to cybersecurity.

2. *Raj Chaudhary and Jared Hamilton. "What You Need to Know to Demystify Cybersecurity." Crowe Horwarth, October 2014. http://www.crowehorwath.com/folio-pdf/WhatYouNeedtoKnow DemystifyCybersecurity_RISK15905.pdf*

Figure 9. Percentage of respondents who indicate the following obstacles very much or extremely affect internal audit's ability to address cybersecurity risk.



Note: Q5: Rate the degree to which each of the following obstacles affects internal audit's ability to address cybersecurity risk.

Training on this approach — complemented with additional training in specific areas such as the organization and processes involving information security and privacy, social engineering, phishing schemes, and the importance of complex passwords — would empower auditors to perform cybersecurity assurance work more effectively.

In addition to a lack of cybersecurity expertise, a noticeable percentage of respondents also noted lack of cooperation from IT, lack of support from executive management, or lack of understanding of cybersecurity among board members as factors that very much or extremely affect internal audit's ability to address cybersecurity risk.

The time to change the conversation has come. CAEs should address the increased likelihood of a cybersecurity breach by enhancing the organization's cyber resiliency. To move into this potentially unfamiliar — and perhaps uncomfortable — territory, internal audit needs to obtain the necessary talent. As noted with addressing culture, however, success does not depend solely on having the right technical skills. Ultimately, the success of these efforts depends in large part on obtaining the support

and cooperation of key players: IT, executive management, and the board. CAEs need to have the right interpersonal skills and relationships to ensure support and cooperation.

Next Steps for the CAE

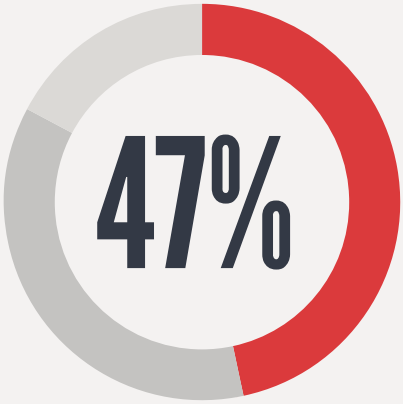
- Understand cybersecurity risk, its components, and complexities.
- Understand the extent and maturity of cyber resiliency of the organization considering all aspects: protection, monitoring, response, and recovery.
- Adjust audit plan activities to capture cyber resiliency aspects.
- Ensure internal audit has the skills to be engaged with risks around cybersecurity and resiliency activities.
- Assess the readiness of the organization to limit the impact of an intrusion.
- Assess the ability of the organization to provide the appropriate level of required response and recovery activities to ensure a smooth transition back to full business operations.
- Discuss the level of cyber resiliency preparedness with management and the audit committee.

Assessing Involvement in Organizational Use of Data

USE OF DATA IS GROWING. IS INTERNAL AUDIT SUFFICIENTLY INVOLVED?

Reported that internal audit is very or extremely involved in evaluating the quality of data used in their organization.

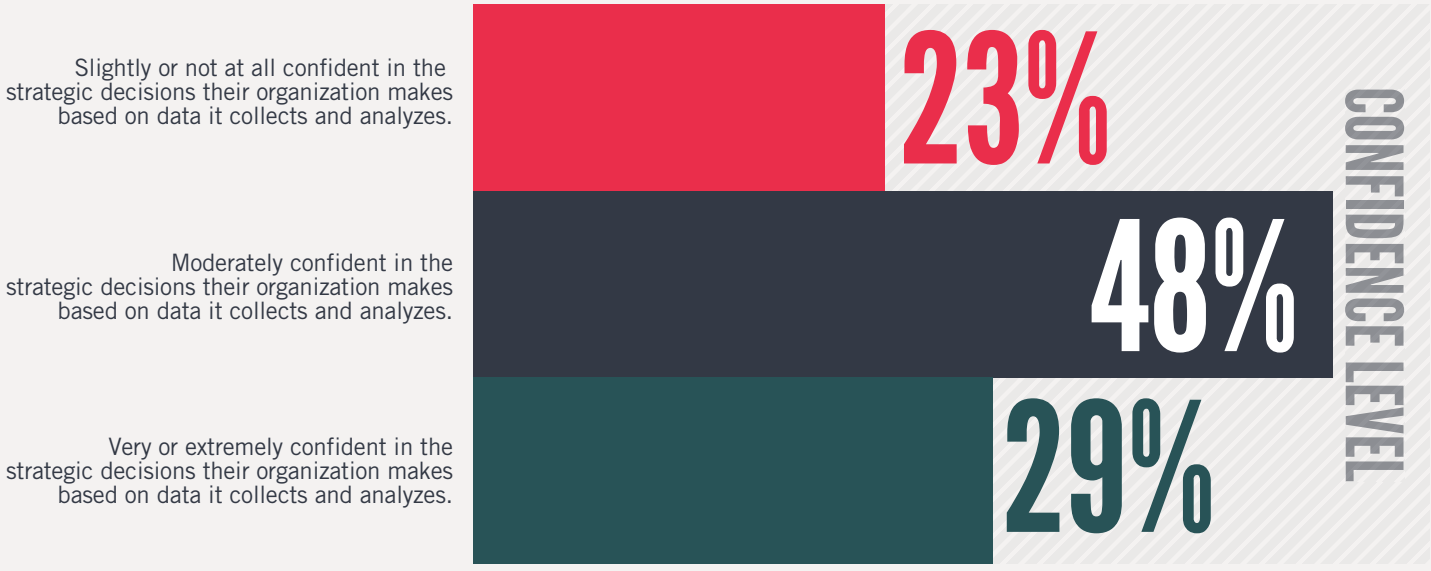
Reported that internal audit is moderately involved in evaluating the quality of data used in their organization.



Reported that internal audit is slightly or not at all involved in evaluating the quality of data used in their organization.

37% indicated that data mining and analytics skills are very or extremely essential to their internal audit function's ability to perform its responsibilities.

CAEs LACK CONFIDENCE IN ORGANIZATIONAL USE OF DATA...



ASSESSING INVOLVEMENT IN ORGANIZATIONAL USE OF DATA

Imagine a time when your eligibility to receive health services is completely automated, a time when a computer system applies algorithms to determine the kind of care you receive. What if the measurements involved in these calculations are incorrect? How will that affect your eligibility? This scenario is not far from reality. Presently, insurance premiums are calculated based on several factors that define the risk level of a particular group. As more types of data can be gathered, organizations of all sorts are relying on data to make decisions.

The power data has to inform decisions comes with the potential to misdirect organizations. Problems can arise from data collection, data analysis, and decisions made from the data. For example:

- Is collection and use of the data legal and ethical?
- Has the organization confirmed the data's appropriateness, accuracy, and completeness? Data often contains gaps and inaccuracies.
- Was the right expertise involved in evaluating the data to ensure the evaluation is not biased or flawed? The difference between correlation and causation is not always well understood.
- Are conclusions drawn from the data based on what the data proves or what someone wants the data to prove?

The questions above put in perspective the range of risks present with an organization's use of data. Consider such concerns along with the increasing availability of data and sophistication of the tools available to analyze data, and one could conclude that the risk for many (if not most) organizations related to their collection and use of data is greater than it was even a few years ago.

With the expertise in data analytics that exists in many internal audit departments, CAEs have the opportunity to move the profession into this increasingly risky area by providing assurance over organizational use and evaluation of data. However, the results from the Pulse survey indicate this may be a missed opportunity for internal audit to add value to their organizations. The majority of respondents are neither significantly involved in evaluating the quality of an organization's data nor are they confident in the strategic decisions made based on that data. Specifically, only 17 percent of respondents reported that internal audit is very or extremely involved in evaluating the quality of data used in their organization (see Figure 10). In addition, only 29 percent are very or extremely confident in the strategic decisions their organizations make based on the data it collects and analyzes (see Figure 11).

BIG DATA

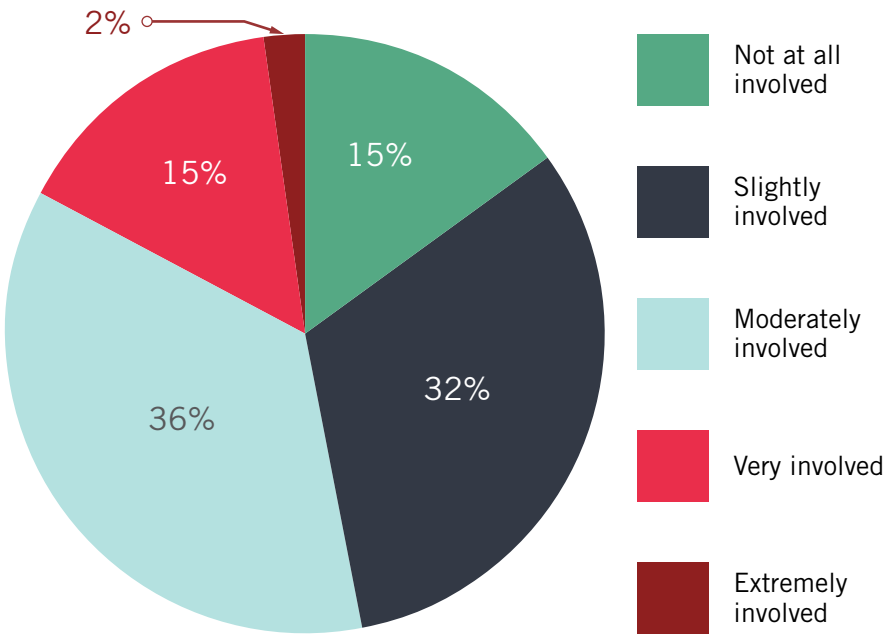
Organizational use of data is not new, but the growing ability to collect and analyze vast quantities of data, Big Data, is changing how organizations make decisions. Big Data is increasingly used by organizations to inform important decisions. There are competing understandings of the phrase Big Data but at the core, the considerations concerning the collection, analysis, and use of data apply to Big Data in a manner that is likely magnified many times over.

THE PROBLEM OF THE THIRD VARIABLE: DRAWING INAPPROPRIATE CONCLUSIONS

If we know drowning deaths increase sharply as ice cream sales increase, can we say ice cream consumption causes drowning? Of course not. That result fails to recognize other facts, such as the effect hot weather has on both ice cream sales and swimming. In other words, just because two things happen together or at the same rate does not mean one caused the other.

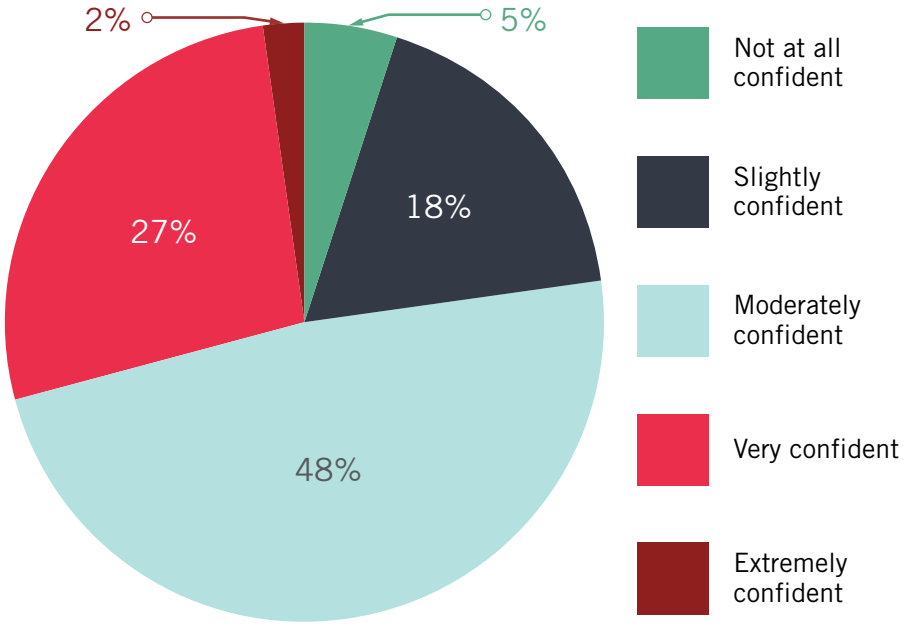
This anecdote points to an important caution: Be careful about drawing conclusions without analyzing and investigating fully all the information and factors involved. And when looking at data-driven decisions in an organization, drill down to assure the validity of your conclusions.

Figure 10. Internal audit involvement in evaluating quality of data.



Note: Q14: Rate the degree to which internal audit in your organization is involved in evaluating the quality of data used.

Figure 11. Internal audit confidence in strategic decisions based on data.



Note: Q15: Rate your level of confidence in the strategic decisions your organization makes based on data it collects and analyzes.

REINVESTING IN A CORE SKILL: DATA ANALYTICS

CAEs may be underestimating the value of internal audit's data mining and analytics skills. Industry is at a threshold of significant change driven by the increased volume and use of data by organizations. Internal audit's experience with and understanding of data — combined with business acumen — can provide needed assurance.

To get into this space, CAEs may need to reevaluate the importance of data analysis skills. Only little more than a third (37 percent) of respondents reported that they consider data mining and analytics skills very or extremely essential. In contrast, 83 percent of respondents reported business acumen skills as very or extremely essential. When it comes to dealing with the risks of data, both are critical.

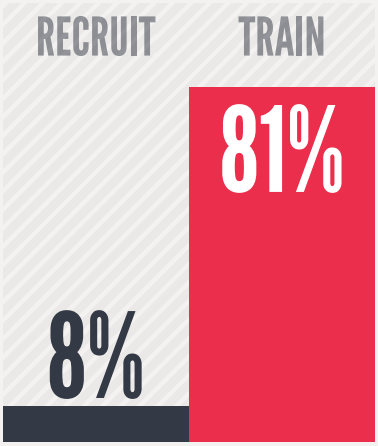
What data an organization collects, how they collect it, how they handle it, how they analyze it, and how they use it are all critical. While it is true these are not necessarily new risks, the increasing amount of data and sophistication of its analysis and use mean these risks are growing quickly in many organizations. Internal auditors need to understand the risks associated with an organization's use of data, prepare for them, and address them.

Next Steps for the CAE

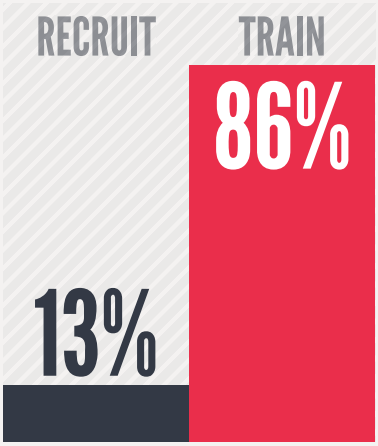
- Understand the nature and extent of data used by the organization.
- Assess the risk of data collection, processing, handling normalization, and data analysis based on its sensitivity, importance, and impact on the organization's key activities.
- Discuss with management and the audit committee the risks to the organization from data use, such as risks to security and privacy. Add specific elements to the audit plan addressing these risks.
- Ensure internal audit has the skills to be engaged with the risks around the increasing use and sophistication of data.

Valuing Interpersonal Skills

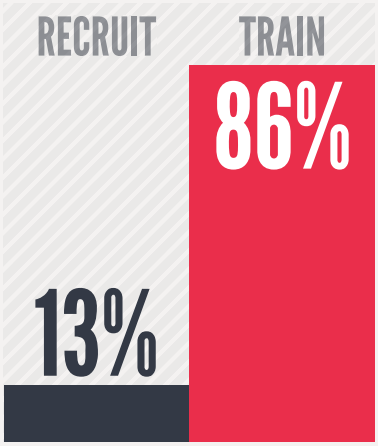
HOW ARE CAEs DEVELOPING THEIR TEAM'S SOFT SKILLS?



Accounts for the organization's politics.



Balances diplomacy with assertiveness.



Manages conflict effectively.

AMONG RESPONDENTS WHO REPORTED TRAINING INTERNAL AUDIT STAFF ON SOFT SKILLS...

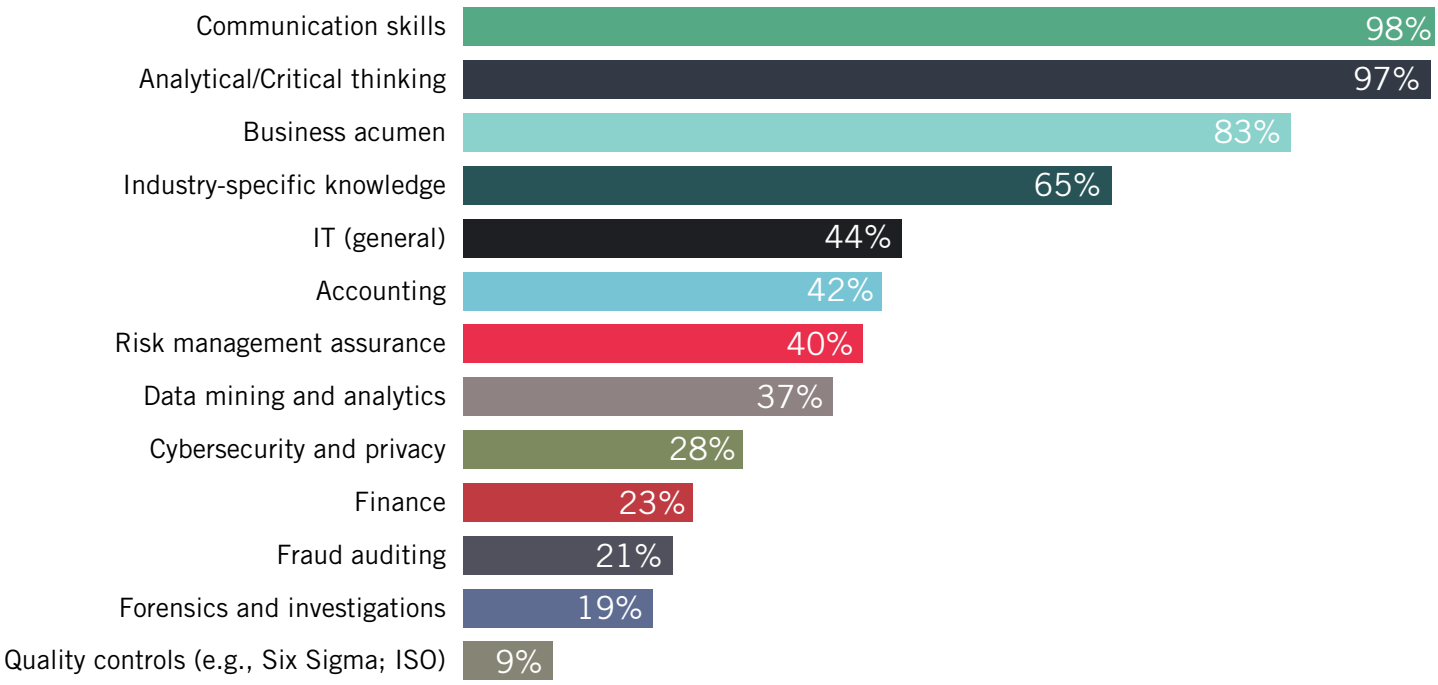
Classroom Training	**3%** Accounts for the organization's politics.	**8%** Balances diplomacy with assertiveness.	**19%** Manages conflict effectively.
Informal Training	**94%** Accounts for the organization's politics.	**88%** Balances diplomacy with assertiveness.	**78%** Manages conflict effectively.
Training moderately or less effective	**55%** Accounts for the organization's politics.	**56%** Balances diplomacy with assertiveness.	**58%** Manages conflict effectively.

VALUING INTERPERSONAL SKILLS

If internal audit seeks to move more into the role of trusted adviser, addressing challenging topics such as culture and cybersecurity, interpersonal skills need to be stronger. For some internal auditors, focusing on skills such as active listening, effective communication, and diplomacy may be new and uncomfortable, but they are necessary to meet the growing expectations of internal audit as it engages in emerging risks.

CAEs and directors who responded to the Pulse survey agree that soft skills are vital. An overwhelming majority consider communication and business acumen skills very or extremely essential (see Figure 12). Yet when asked about the proficiency of specific soft skills, only a fair to middling number of respondents rated their team as very or extremely proficient. In general, respondents rated their average team member as only moderately proficient in most soft skills. For example, 48 percent rated their average team member as moderately proficient in managing conflict effectively, and an additional 15 percent rated their average team member as slightly or not at all proficient in this skill. Similarly, 44 percent rated their average team member as moderately proficient in accounting for an organization's politics, and an additional 21 percent rated their average team member as slightly or not at all proficient in this skill. (See Figure 13.)

Figure 12. Percentage of respondents indicating skills are very or extremely essential.



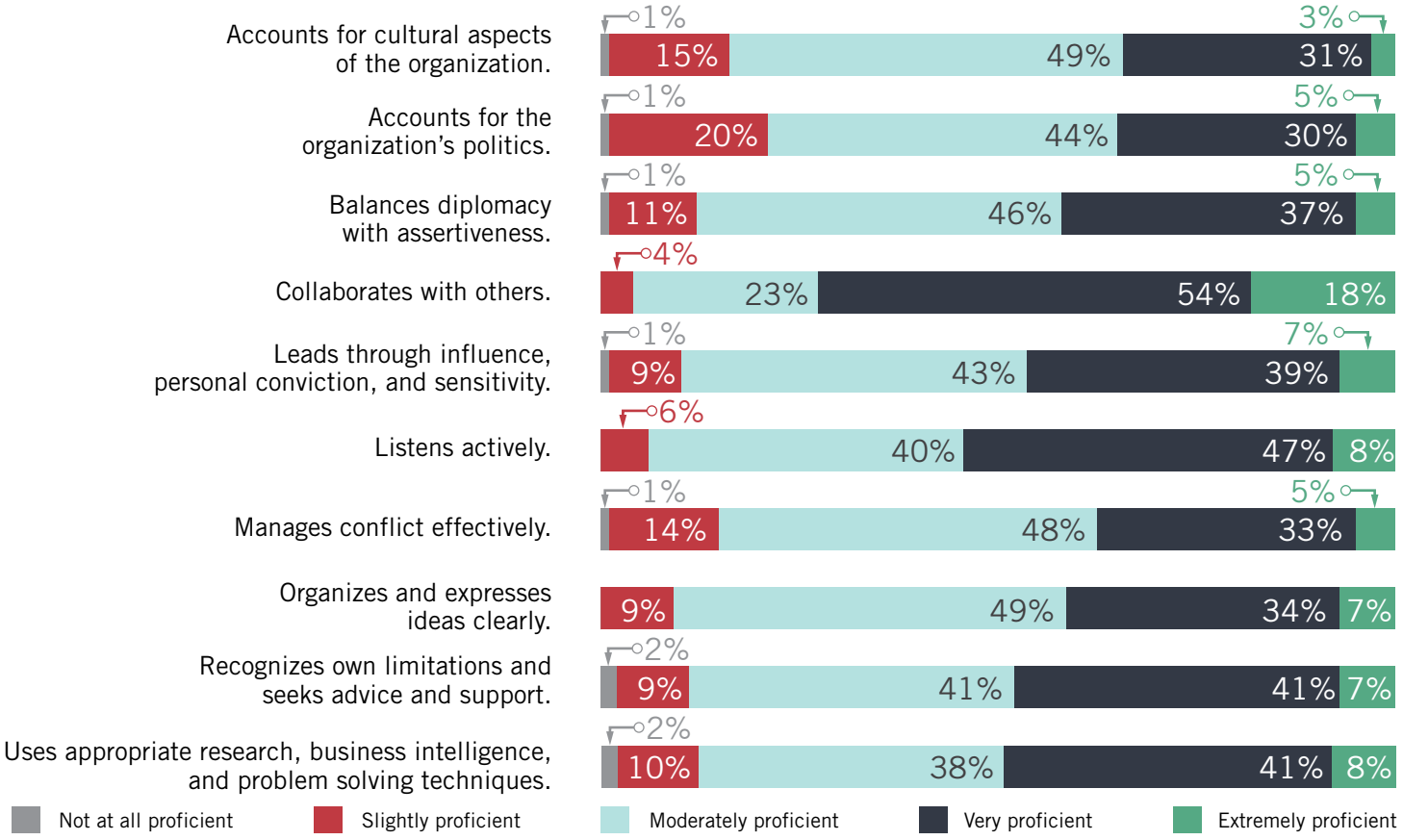
Note: Q27: For each of the skills listed, please indicate to what degree it is essential to your audit function's ability to perform its responsibilities.

A BRIEF GUIDE TO BUILDING RAPPORT

Whether conducting an investigation or communicating audit findings, internal auditors need to employ basic relationship skills to obtain the trust and confidence of those around them. One such skill is building rapport, which can be further broken down:

- Maintaining appropriate eye contact — most people in the United States relate attentiveness and respect with direct eye contact. At the same time, unwavering eye contact can be unnerving, provoking a person to look away from a direct gaze.
- Verbally tracking the content of a person's speech — natural discourse includes verbal signals that the listener is following the speaker accurately. Such acknowledgment generally leads to greater disclosure.
- Matching vocal tone and tempo — a mismatch between verbal styles can make a person feel rushed or uneasy.
- Body language — when rapport is established, people will unconsciously mimic each other's body movements. Conversely, an abrupt change in body language may indicate a disruption to the rapport built.

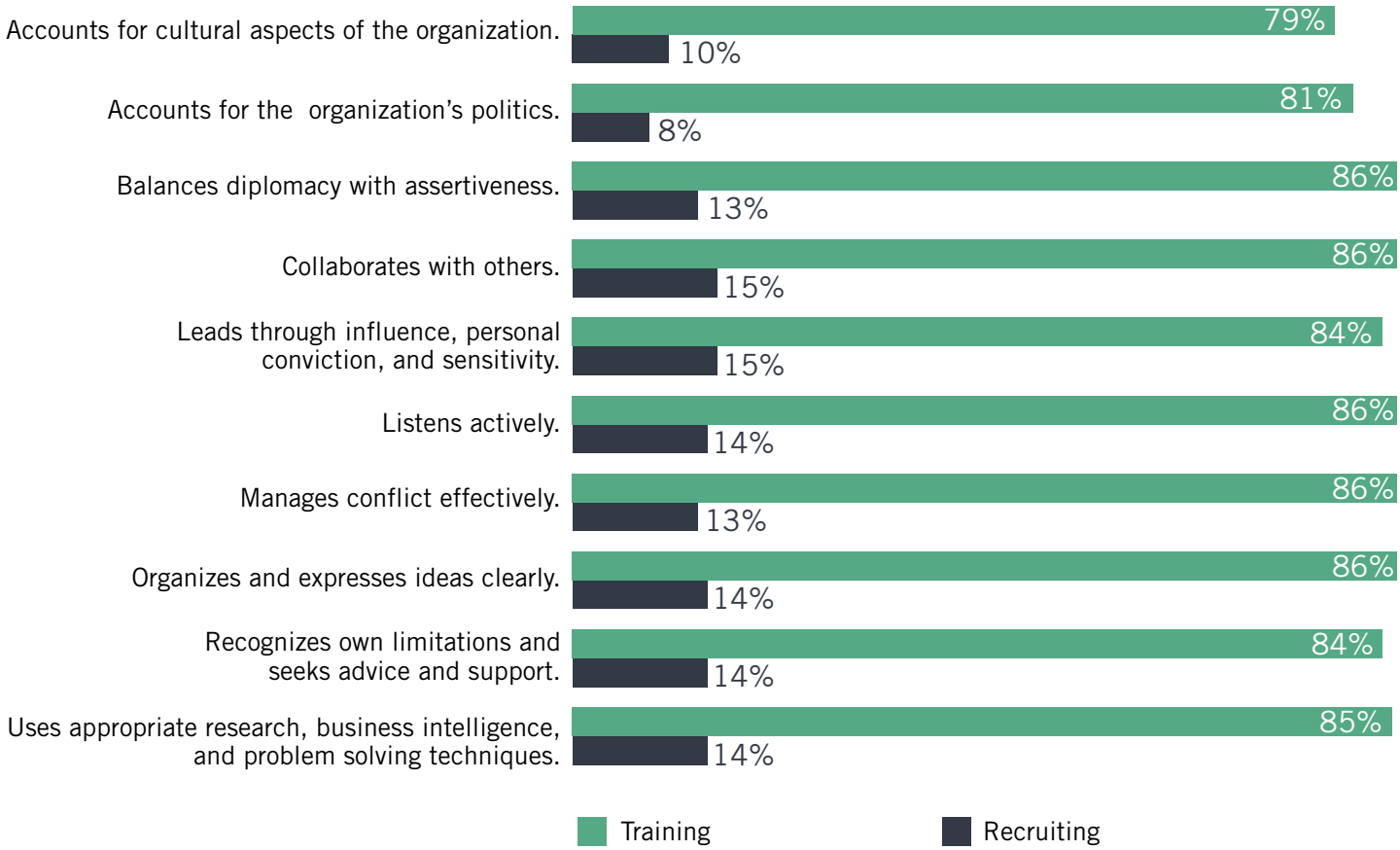
Figure 13. Soft skills proficiency of average team member.



Note: Q31: Rate the proficiency of the average member of your audit team for the following skills. Totals do not equal 100 percent due to rounding.

Surprisingly, low numbers of respondents are recruiting for soft skills. Between 8 percent and 15 percent of respondents reported recruiting for any of the soft skills listed in the survey. Recognizing the need for soft skills, upward of 80 percent reported instead that they are training their team for most of the soft skills listed. (See Figure 14.) Those that reported training their team on soft skills rarely use formal training methods. More than 70 percent reported using informal training methods of on-the-job experiences and mentoring for all but one of the listed soft skills (see Figure 15).

Figure 14. Comparison of recruiting versus training soft skills.



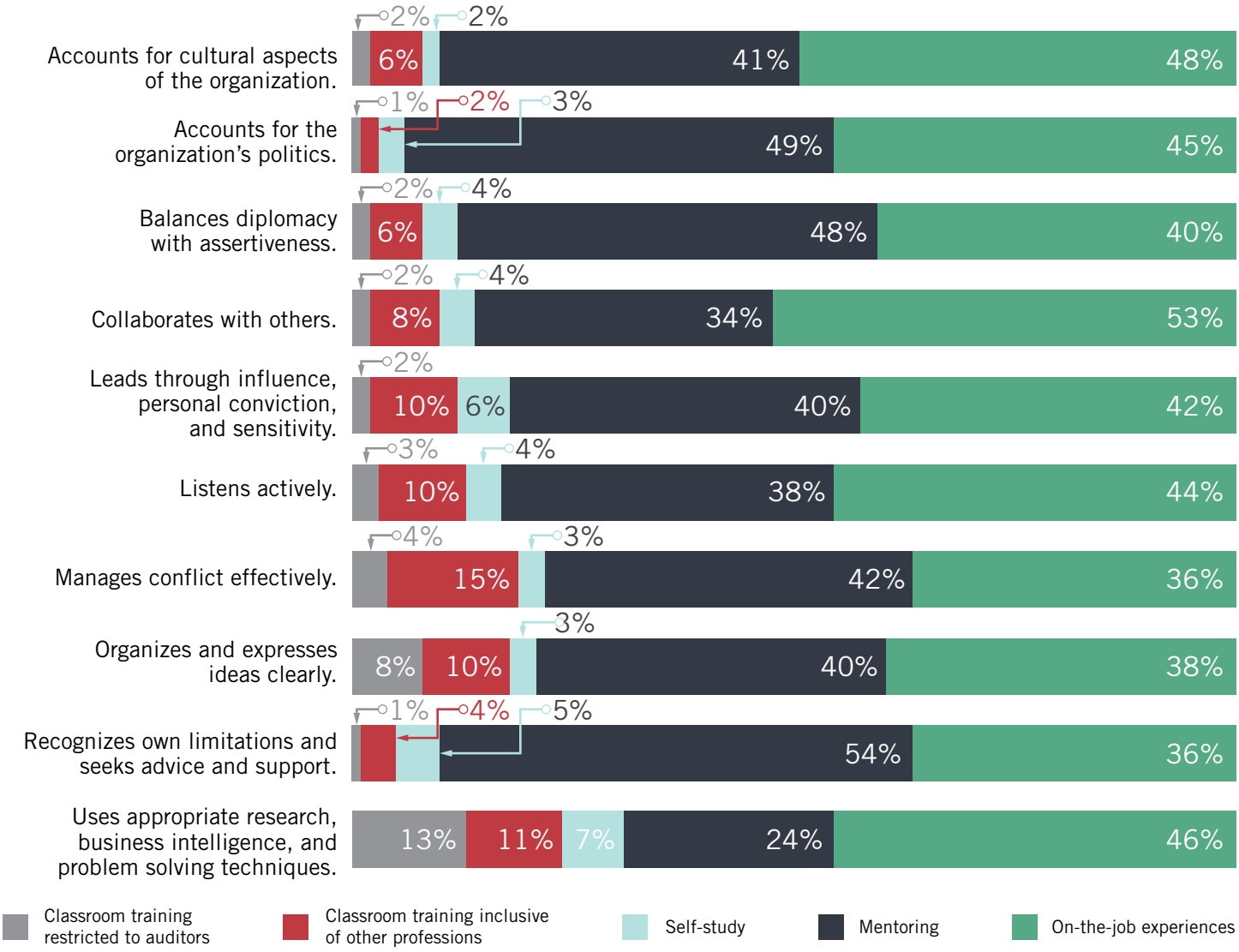
Note: Q30: Indicate if your internal audit function is currently lacking, building/recruiting, and/or training for the following skills. Please also indicate the skills for which you are outsourcing and/or having difficulty hiring. Participants selected all that applied.

Soft skills are apparently difficult to teach. For most soft skills, the majority of respondents rated the effectiveness of their training no better than being moderately effective (see Figure 16). Many cannot identify the individual skills involved in effective interpersonal activity. Even fewer may be self-aware enough to regulate their

own verbal and nonverbal communication to achieve a desired effect. As such, it is not surprising that efforts to train internal audit professionals informally have resulted in moderate levels of proficiency at best.

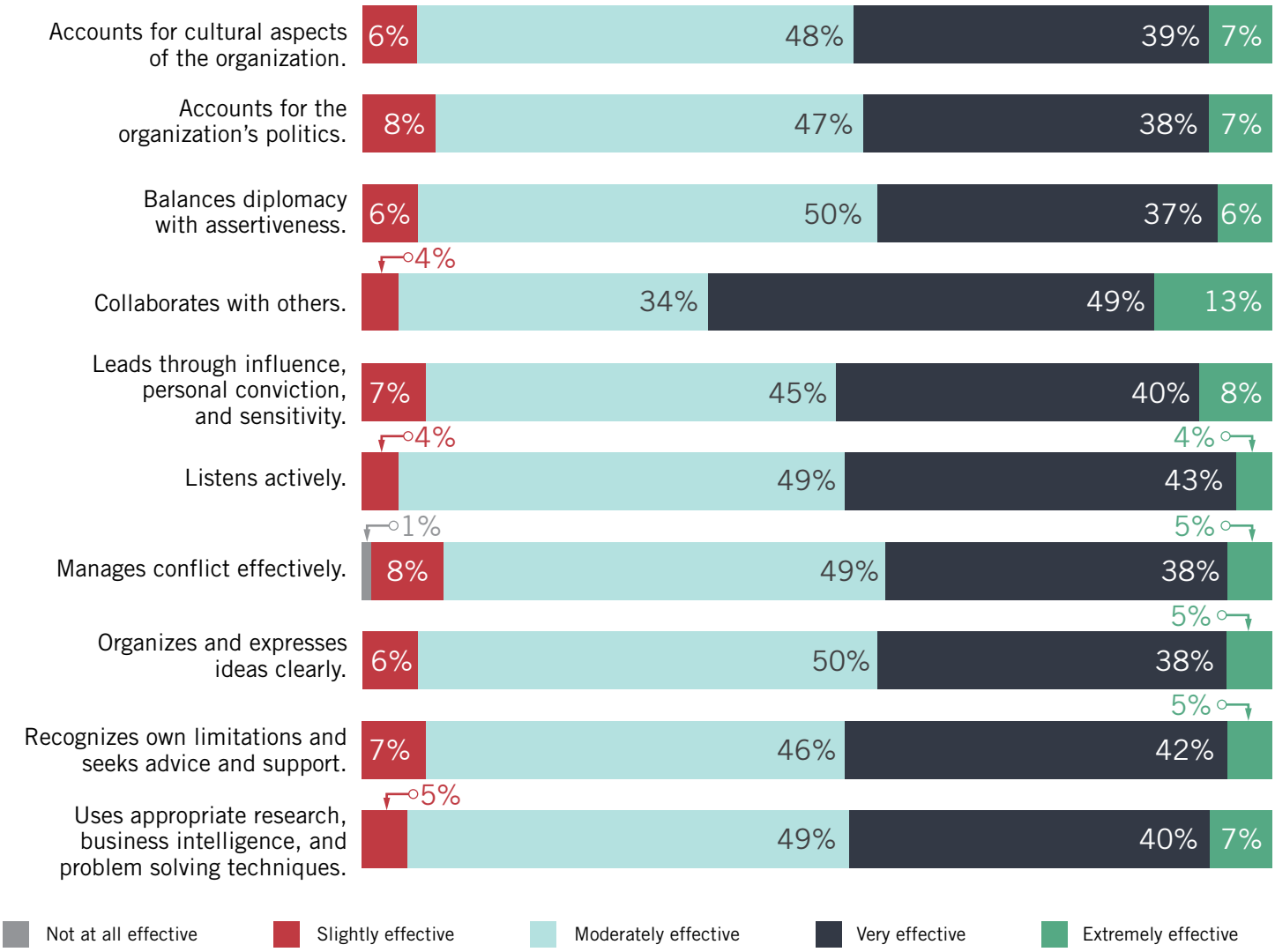
Despite changes in responsibilities, the stated skills requirements for internal audit professionals do not seem to have kept up. Even though financial audits, including Sarbanes-Oxley, represent less than 20 percent of the average audit plan as reported in the survey (see Figure 17), a quick review of internal audit postings reveals that

Figure 15. Soft skills training methods.



Note: Q30.1: How are you currently training your staff in the following skills? Includes only respondents who indicated that they trained staff on the specific soft skill. Excludes responses of "Other" and "N/A." Totals may not equal 100 percent due to rounding.

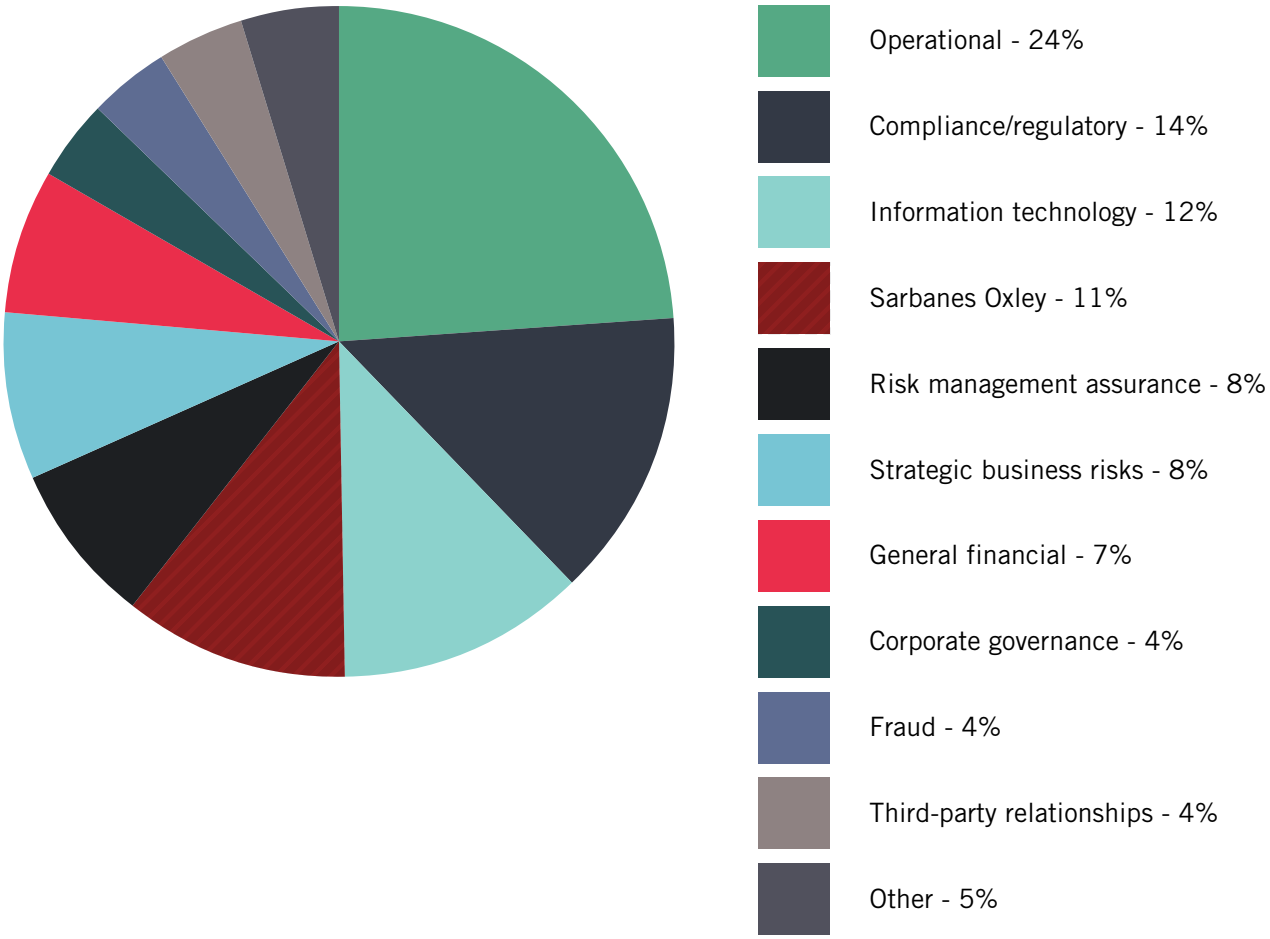
Figure 16. Effectiveness of soft skills training methods.



Note: Q30.2: Rate the level of effectiveness of your training efforts for the following skills. Includes only respondents who indicated that they trained staff on the specific soft skill. Excludes responses of "Other" and "N/A." Totals may not equal 100 percent due to rounding.

such positions often require degrees in accounting or finance with a CPA preferred. Although the hiring trend has increasingly been to consider alternative qualifications, these traditional requirements remain an obstacle to attracting diverse talent. The data from the Pulse survey indicates the essential skills needed for internal auditors today include communication, business acumen, and other soft skills much more often than accounting or finance expertise. As such, CAEs may benefit from doing something different when it comes to talent management.

Figure 17. Average audit plan coverage.



Note: Q22: Looking ahead to next fiscal year, what percentage of your audit plan do you anticipate will be allocated to each of the following risk categories. Total does not equal 100 percent due to rounding.

Consider how an auditor with an engineering background could improve the department's understanding of risks involved at a manufacturing plant. Experience in statistics or a degree in math may enhance the data analytic skills in the department. A background in behavioral or organizational psychology may add needed forensic skills.

Since hiring new talent is not always the best or only answer, take the advice offered by Larry Harrington, 2015–16 global chair of The IIA board and CAE for Raytheon Company, to "invest in yourself" and expand it to your team by bringing in experts to train staff in soft skills rather than relying predominantly on informal training and accepting mediocre results.

Next Steps for the CAE

- Leverage The IIA's Global Internal Audit Competency Framework to help determine the depth and breadth of skills required for internal audit to be successful in your organization.
- Assess the skills of current staff against these requirements.
- Identify skill gaps, prioritizing those that need to be addressed immediately over those that can be addressed over time.
- Determine appropriate training or recruitment needed to address skill gaps. Consider branching out from predominantly informal training methods for soft skills and consider other options that may improve the effectiveness of the training.
- Evaluate current job descriptions to determine whether they reflect the skills needed to address the changing requirements of the internal audit function.

Conclusion

CONCLUSION

The environment is rapidly changing. This year's Pulse continues the journey that began when the 2015 report noted the need for internal auditors to adapt to the volatility of emerging risks. The situation has not stabilized in 2016. Internal audit is at a critical juncture, faced with a choice either to remain in familiar and predictable areas traditionally identified as internal audit's domain or to step out of the comfort zone to confront emerging and unfamiliar risks.

Internal audit has a critical role in the governance of an organization. Our stakeholders expect us to fulfill that role. The perception of some stakeholders is that internal auditors lack the ability to expand their perspective beyond traditional areas as highlighted in KPMG'S 2014 Global Audit Survey. An upcoming CBOK Stakeholder report from The IIA's Research Foundation confirms that the majority of internal audit stakeholders want internal audit to have a more active role in assessing and evaluating strategic risks.

CAEs need to increase focus on the areas of concern among stakeholders, those areas outside of their comfort zone. Doing so moves beyond rebranding internal audit into fundamentally changing the makeup of internal audit. To address emerging risk areas such as cybersecurity, organizational culture, and the organization's use of data, internal audit must invest in audit staff to enhance soft skills.

It is time for internal audit to move beyond being capable of handling old risks and align with the strategic objectives of the organization, stepping into the role of trusted adviser. For many, this requires a shift in mindset from auditing what is comfortable to auditing what is critical. As current risks evolve and new risks emerge, a sense of urgency to audit at the speed of risk is vital to meet and exceed the needs of key stakeholders.

Demographics & Trending Data

Demographics

19 INDUSTRIES REPRESENTED

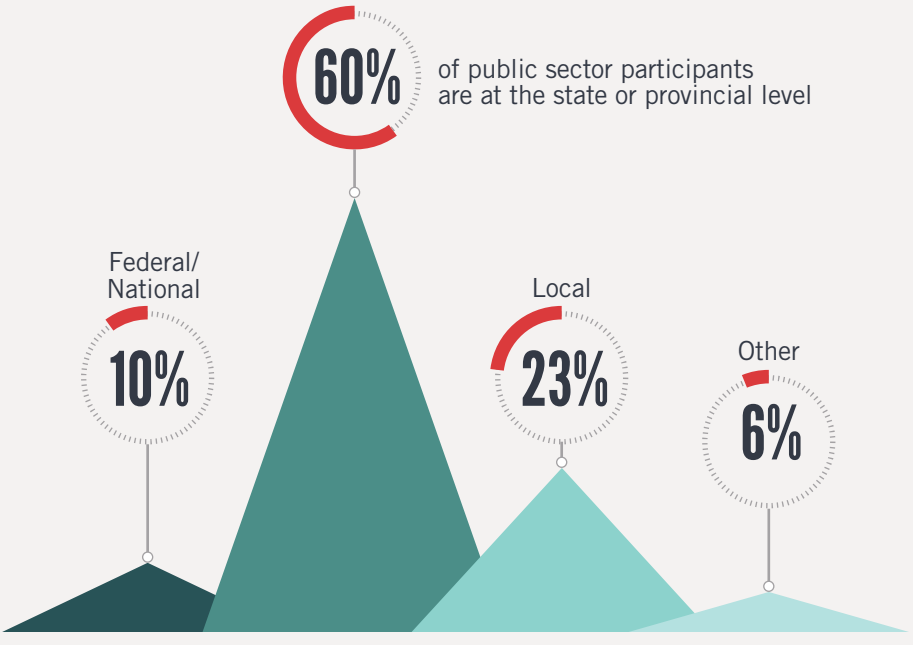
- Finance & Insurance 32%
- Educational Services 10%
- Manufacturing 9%
- Public Administration 8%
- Health Care & Social Assistance 7%
- Utilities 5%
- Retail Trade 4%
- Other 25%

486 CAE AND DIRECTOR PARTICIPANTS

PARTICIPANTS BY ORGANIZATION TYPE

33% of participants from publicly traded organizations are

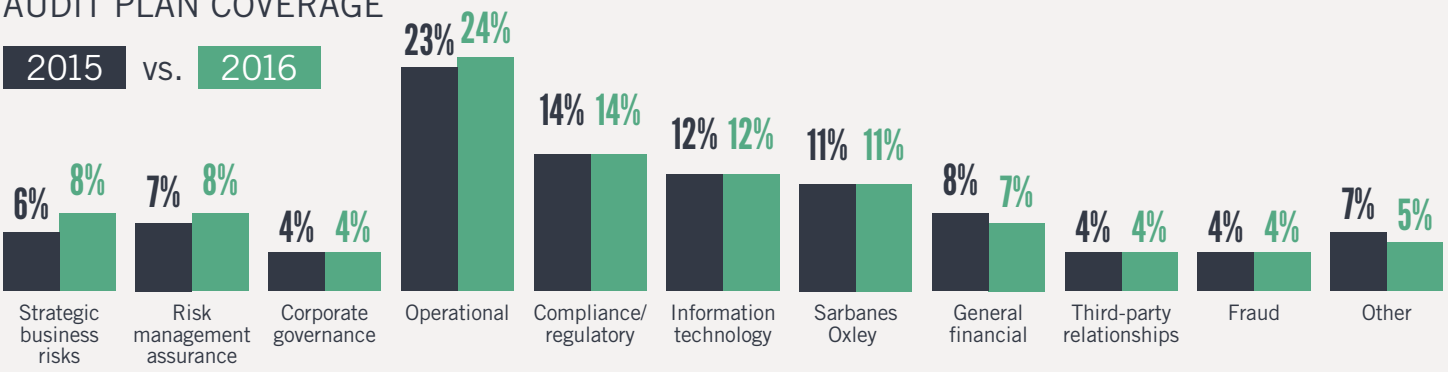
FORTUNE 500



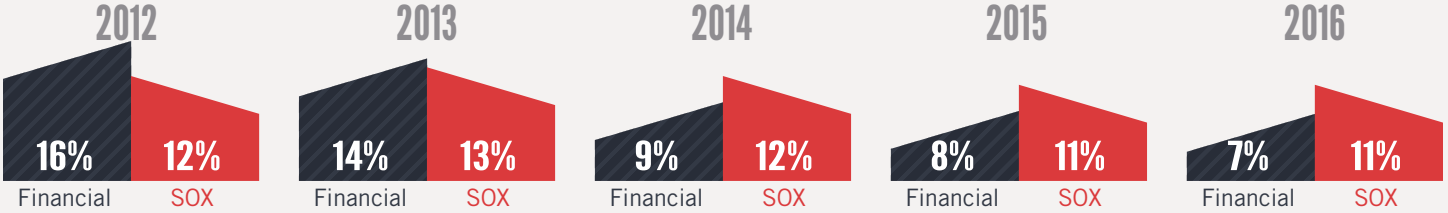
Trending Data

AUDIT PLAN COVERAGE

2015 vs. 2016



PLAN COVERAGE FOR FINANCIAL AUDITS



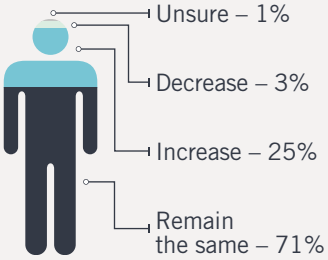
CAE ADMINISTRATIVE REPORTING LINE

	2013	2016
Chief financial officer (CFO)	37%	35%
Chief executive officer (CEO)	33%	35%
Audit committee or board of directors	10%	9%
General or legal counsel	6%	6%
Chief compliance officer (CCO)	2%	2%
Chief risk officer (CRO)	2%	3%
Other or N/A	10%	10%

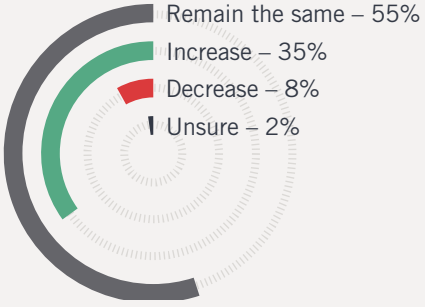
CAE FUNCTIONAL REPORTING LINE

2013	2016	
76%	83%	Audit committee or board of directors
10%	9%	Chief executive officer (CEO)
6%	5%	Chief financial officer (CFO)
<1%	<1%	General or legal counsel
<1%	<1%	Chief compliance officer (CCO)
0%	0%	Chief risk officer (CRO)
6%	2%	Other or N/A

INTERNAL AUDIT STAFFING PROJECTION



INTERNAL AUDIT BUDGET PROJECTION



The Institute of Internal Auditors

Audit Executive Center®

GLOBAL HEADQUARTERS
247 Maitland Avenue
Altamonte Springs, FL 32701-4201
www.globaliia.org

2016-2113