2019 NORTH AMERICAN PULSE OF INTERNAL AUDIT

Defining Alignment in a Dynamic Risk Landscape

The Institute of Internal Auditors

AUDIT EXECUTIVE CENTER

About the Pulse of Internal Audit

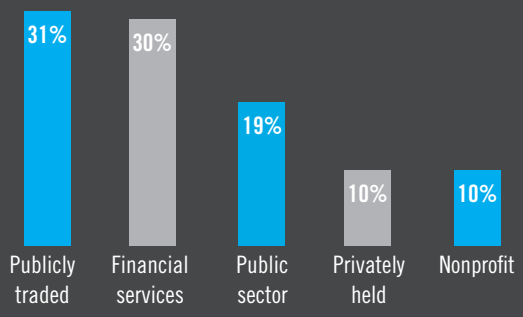
NUMBER OF RESPONSES	
CAEs	447
Directors/senior managers	65
Total	512

The IIA's Audit Executive Center® (AEC®) has gathered insight from leaders in the profession through the annual Pulse of Internal Audit survey (Pulse) since 2011. Each survey collects information about both established and emerging issues that are important to the profession as well as information about internal audit management (such as audit plan allocations and staff level changes).

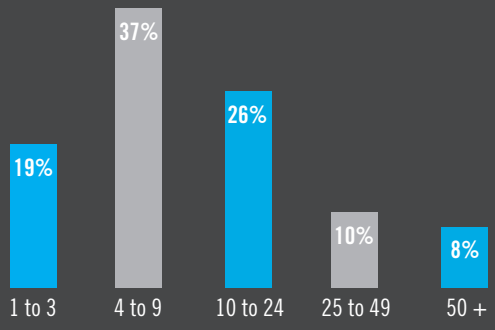
The online survey for the North American Pulse 2019 report was conducted from Sept. 5 to Oct. 4, 2018. Respondents primarily come from the United States (85 percent) and Canada (10 percent) with the remainder coming from a variety of other countries. For analysis, financial services respondents are separated from other organization types into a separate category (as shown in the graph below).

The survey results are analyzed and presented in multiple reports, some of which are made available to the public through The IIA's Pulse of Internal Audit resource page (visit www.theiia.org/Pulse). More in-depth reports are available exclusively to members of the AEC. For more information about joining the AEC, visit www.theiia.org/AEC.

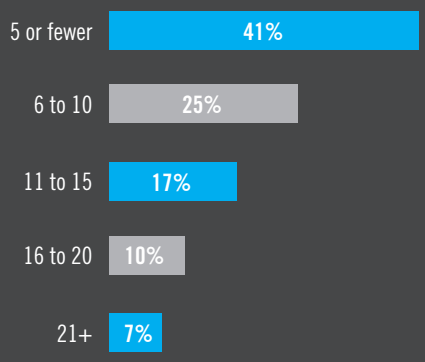
Organization Type With Financial Services Breakout

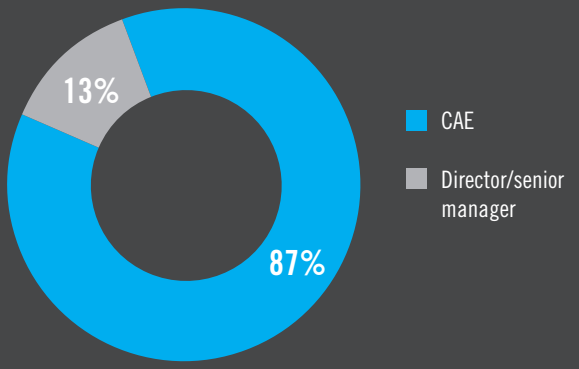


Internal Audit Function Size (Full-time Employees)



Years of CAE/Director Experience





Contents

ABOUT THE AUDIT EXECUTIVE CENTER

The IIA's Audit Executive Center® (AEC®) 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/AEC.

ABOUT THE IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla. For more information, visit www.theiia.org.

DISCLAIMER

COPYRIGHT

Executive Summary

Over the past decade, the speed at which risks emerge and evolve has accelerated dramatically, compelling organizations to adopt new strategies and reorder priorities to survive and thrive in an increasingly complex risk environment.

Today's board members and senior executives must be mindful of a dizzying array of factors, such as disruptive technologies, geopolitical uncertainty, and global economic conditions that threaten to derail organizational goals. The increasing complexity of such daunting challenges makes it imperative for all players in risk management to be informed and aligned.

Boards are responding by adding cyber savvy members and demanding better information on risk management from executive management, especially with regard to cybersecurity. They also are aware that they must improve their own understanding of the impact of risks and opportunities. Strengthening oversight of strategy execution and risk management are top improvement priorities for boards, according to the 2018–2019 Public Company Governance Survey conducted by the National Association of Corporate Directors (NACD).[1]

Boards and executive management continue to support internal audit as a risk management partner as reflected in continuing growth in internal audit staff sizes. More than twice as many CAEs reported increases versus decreases in staff size in 2018 (26 percent with increases vs. 11 percent with decreases). The most growth was with functions with 10 to 15 FTEs, where 35 percent reported increases compared to 6 percent with decreases.

Alignment with board and executive management views on risk is essential for internal audit to successfully provide outstanding service and be viewed as a value-added and essential resource. Not only must internal audit be thoroughly and continuously aligned with the board and executive management, it is imperative for practitioners to be cognizant of whether and how these stakeholders view and understand risks and opportunities. This begins and ends with assuring that boards have complete and accurate information on which to base their decisions. Internal audit leaders must be prepared to lead discussions if management lags on addressing certain risks and have the courage to speak up if management is not properly focused.

Since 2011, the North American Pulse of Internal Audit has provided CAEs and other internal audit leaders with practical direction on vital issues facing the profession. The 2019 report aims to provide insights and direction to help internal audit inform and influence boards and executive management in four key risk areas: **cybersecurity and data protection, third-party risks, emerging and atypical risks,** and **board and management activity.**

Data from this year's survey, which included input from more than 500 internal audit executives, suggest potentially troubling misalignment in the risk areas of focus in this report and a need for CAEs to elevate these concerns to the audit committee.

Cybersecurity and Data Protection

While cyber and IT issues have grown to represent nearly 20 percent of the average audit plan, individually these key issues continue to lag behind others considered lower risks by boards, such as operational, financial reporting, and compliance/regulatory (Exhibit B). Additionally, CAEs report slow progress in building IT and cyber skills among their staffs, and an effort gap is developing between the effort internal audit functions deliver on cybersecurity and the level CAEs believe they should provide. One potential action item is for CAEs to leverage boards' increasing interest and involvement in cybersecurity issues to discuss adjustments to audit plan allocations and resources and other steps to close any existing effort gaps in this key risk area. Additionally, CAEs must look at all options, including cosourcing, to strengthen cyber skills on their staffs. Candid discussions with the audit committee about obstacles to internal audit's performance ensure the issues are on the record in the event a future cyber issue arises.

Third-party Risks

Organizational monitoring of third-party relationships is viewed by nearly half of CAEs as ad hoc or weak. Survey responses clearly indicate CAE concern about how third parties are selected and monitored (Exhibit 5), and how ill-prepared organizations are for managing poorly performing vendors (Exhibit 6).

A recommended action item is for CAEs to educate stakeholders that third-party relationships are part of the organization's ecosystem of risk and cannot be viewed as separate. What's more, CAEs must elevate concerns about weak controls on third-party risks to the audit committee. These relationships require the same level of risk management as any that affect the organization directly.

Emerging and Atypical Risks

CAEs report that boards are much more likely to turn to management than internal audit to identify and assess emerging or atypical risks (Exhibit 11). While most CAEs express strong confidence in their organizations' abilities to identify and assess such risks, nearly half say it is fairly common that an emerging or atypical risk will surprise management in the course of a year (Exhibits 8, 9, and 10).

Alerting boards of a potential misalignment on emerging and atypical risks is a first step in opening the door to internal audit taking on a greater role in these key risk areas. CAEs should advocate for monitoring key risk indicators (KRIs) that include precursors to emerging risks.

Board and Management Activity

More than half of respondents say internal audit rarely or never provides assurance on information that management provides to the board (Exhibit 15). At the same time, board members say the quality of information from management must improve, according to the 2018–2019 NACD Public Company Governance Survey.[2] What's more, variations in committee responsibilities may be hampering internal audit findings and insights from reaching the board in key risk areas, such as cybersecurity.

CAEs should be prepared to provide assurance on information going to the board and push to attend/participate in other key board committees, such as IT, risk, or compensation committees, to ensure internal audit's views are clearly communicated to the board.

Using This Report

By leveraging insights from this year's Pulse, CAEs can better inform stakeholders about potential underperformance in these key risk areas and take advantage of recommended strategies for identifying and addressing any areas of weakness or misalignment that may exist in their organizations. By having the discussion with the audit committee, concerns are put on the record for action. As in previous years, the survey results also offer valuable benchmarking information on audit plans, staffing, and outsourcing (see Appendix, "Internal Audit Management Metrics"). The report this year also features three-year audit plan trends with breakouts by organization types.

Any area of misaligned risk not only presents clear risks to the organization, it can also undermine the confidence in internal audit should things go awry. As is often the case in times of crisis, internal audit falls victim to the inevitable question of "Where were the internal auditors?" CAEs can protect against such criticism by raising their voices when misalignment or control weaknesses go unaddressed or when new risks are not properly addressed. After all, a risk not communicated is a risk assumed.

Introduction

a·lign·ment: *A position of agreement or alliance*

Discussions about aligning internal audit's work with the board's demands typically focus on the CAE's ability to understand the needs of the board and executive management. The common reference to recognizing what keeps stakeholders up at night or what should keep them up at night is a direction for internal audit leaders to know what matters most in boardrooms and C-suites.

This includes understanding the tone and direction set by stakeholders on the balance between opportunities and threats posed by risks. To achieve this, CAEs are urged to learn more about their organizations' industries, hone their business acumen, and build stronger relationships with boards and audit committees, executive management, and other risk professionals within the organization. It also inevitably will require courageous conversations by the CAE.

There are numerous resources available to help CAEs get insight into the board's thinking, including the annual NACD Public Company Governance Survey of board members. For example, the 2018–2019 survey identifies changes in regulatory climate, the prospect of an economic slowdown, growing cybersecurity threats, business-model disruption, and worsening geopolitical volatility as the most significant risks on the minds of board members in 2019. CAEs should be aware of and read the same material that boards and executive management read to keep ahead of the curve.

While the challenge for boards to identify, understand, and react to risk is formidable, boards know risks also offer opportunity. According to the 2018–2019 NACD survey's Key Findings, "Directors rate artificial intelligence (AI) as the biggest technology disruptor, but also regard it as the biggest enabler likely to benefit their organizations in the next 12 months." The CAE, more than ever before, must be aware of and comfortable talking about IT issues and disruptive technology.

To be sure, technology in general has quickened the pace of business advancement and how fast risks emerge and mature. The internet opened the door to a fourth industrial revolution and also introduced the world to cyberattacks. Indeed, the growing challenges related to cybersecurity and data protection have dramatically shifted risk priorities and created new compliance risks, such as new cyber regulations in Europe, the United States, and China. The growing data privacy movement promises to further complicate the technology risk profile and will require greater involvement and assurances from internal audit.

These developments place an even higher value and urgency on assuring that boards have complete and accurate information on which to base their decisions. Internal audit can help fill that role. Just as internal audit's role in the organization is evolving from providing reactive and passive hindsight assurance to one of delivering proactive insight and foresight, so too must its view of alignment reflect the changing needs of the board. In today's dynamic risk environment, CAEs must do more than simply understand and fall in line behind the board's view on risk. This new outlook must center on assuring the board has a comprehensive and unencumbered understanding of the organization's risk universe. This shift in perspective, while subtle, holds great significance in internal audit's ability to provide independent assurance, add value to the organization, and elevate its stature to the level of trusted advisor.

Aligning With the Board and Executive Management

CAEs must seek out any opportunity to educate themselves about board and executive management views on risk to find proper alignment. This starts with continuous conversations between CAEs and their internal audit function's key stakeholders. Communication is vital to maintaining alignment. It also includes leveraging survey data and other resources that provide insight into the bigger picture from board members and executive management and what is influencing their views. There is value to gauging the perspectives of other boards and executive management in other organizations. However, every stakeholder is different; therefore, CAEs must be in tune with the specific perspectives on risk of their board and executive management.

Exhibit 1: Resources for Understanding and Communicating With the Board and C-suite

What the Board and C-suite Are Saying

- Annual Global CEO Survey (PwC)
- Annual Corporate Directors Survey (PwC)
- Executive Perspectives on Top Risks (North Carolina State University's ERM Initiative and Protiviti)
- NACD Public Company Governance Survey (National Association of Corporate Directors)

What They Are Reading

- The Global Risks Report (World Economic Forum)
- NACD Blue Ribbon Commission Report (National Association of Corporate Directors)
- NACD Governance Outlook Report (National Association of Corporate Directors)

What Internal Audit Should Be Sharing

- Pulse of Internal Audit (The IIA)
- Tone at the Top (The IIA)
- Risk in Focus: Hot Topics for Internal Auditors (European Confederation of Institutes of Internal Auditing {ECIIA} and IIA–France {IFACI})

SECTION 1

Cybersecurity and Data Protection

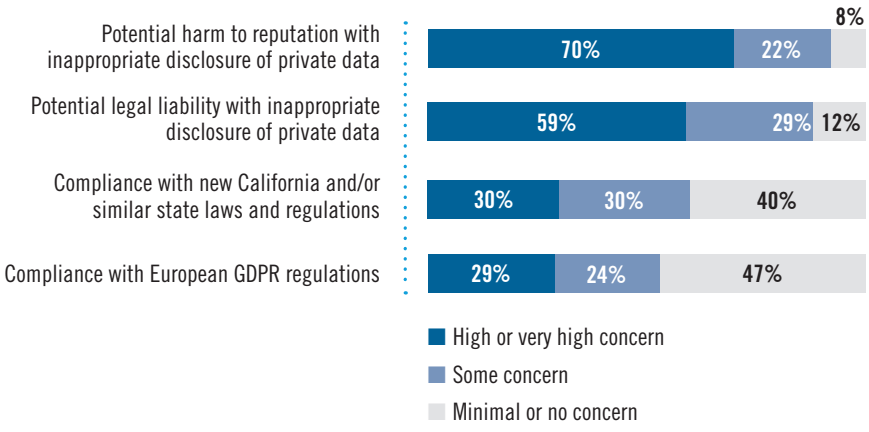
The Pulse survey found that cyber and IT remain top risks among respondents. The greatest concern expressed by CAEs was for potential reputational harm to the organization resulting from an inappropriate disclosure of private data, with 7 in 10 identifying this as an area of high or very high concern within their organizations (Exhibit 2).

This concern reflects alignment with boards, which have consistently identified cybersecurity threats as a top five trend impacting their organizations, according to the 2018–2019 NACD Public Company Governance Survey.[3]

However, concerns regarding compliance with new data protection rules, such as state laws in California and New York or the European Union's General Data Protection Regulation (GDPR) rules, rated as a much lower risk concern, with 47 percent of respondents expressing that their organizations have minimal or no concern regarding the latter (Exhibit 2).

of CAEs identify risk **of reputational damage caused by a privacy data breach** as an area of high or very high concern.

Exhibit 2: Organizational Concerns About Privacy Risks



Note: Q9: Indicate the level of concern within your organization regarding privacy of employee or third-party data maintained by your organization. Those who chose "not applicable" were not included in the analysis for that variable. $n = 407$ to 507.

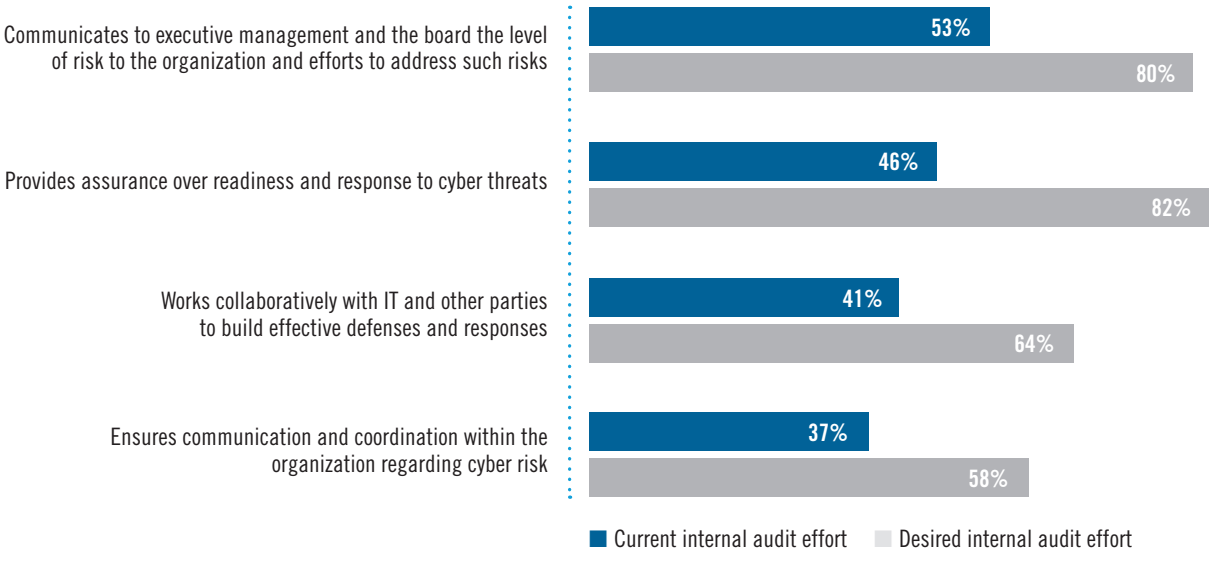
This could reflect some misunderstanding of how and when these new data protection and privacy rules apply. For example, some U.S.-based CAEs may not realize that their organizations are just as responsible for complying with GDPR rules and susceptible to related sanctions as their counterparts in Europe. This is because the rules are not based on the location of the organization, but rather on the location of the customer whose data is being gathered. Any organization that has customers in Europe has an obligation to meet data privacy and protection regulations outlined by GDPR.

However, it should be noted that concern about GDPR compliance skews toward greater concern as the size of the organization grows. For example, in organizations with more than 50,000 employees, 62 percent rated GDPR compliance as a high or very high concern compared to 29 percent who rated it that way overall. This suggests that larger organizations are more likely to have international operations and greater exposure to GDPR rules.

Effort Gap an Area of Concern

Pulse data reflect potentially significant "effort gaps" when it comes to providing assurance over key areas of cybersecurity. The gap is defined as the difference between the level of effort the internal audit function currently delivers in a particular area versus how much the function should provide, as determined by respondents. For example, 46 percent of respondents said they deliver "extreme or significant" effort over the readiness and response to cyber threats, yet 82 percent said they should provide "extreme or significant" effort (Exhibit 3). The effort gap may reflect that internal audit is failing to adapt quickly enough to changing needs and is not able to deliver the necessary assurance. It also suggests that there is a potential misalignment between risk priorities and the audit plan. While cyber and IT issues have grown to represent nearly 20 percent of the average audit plan, individually the two risk areas continue to lag behind issues considered lower risks by boards, such as operational, financial reporting, and compliance/regulatory (Exhibit B in Appendix).

Exhibit 3: Actual vs. Desired Internal Audit Cybersecurity Efforts*



Note: Q6 and Q7: Describe the level of effort an internal audit function "currently has" (Q6) or "should have" (Q7) in each of the following areas in regard to cybersecurity. *Percentages show extremely significant and signficant effort combined. Other response options were moderate, slight, and low. $n = 496$ to 504.

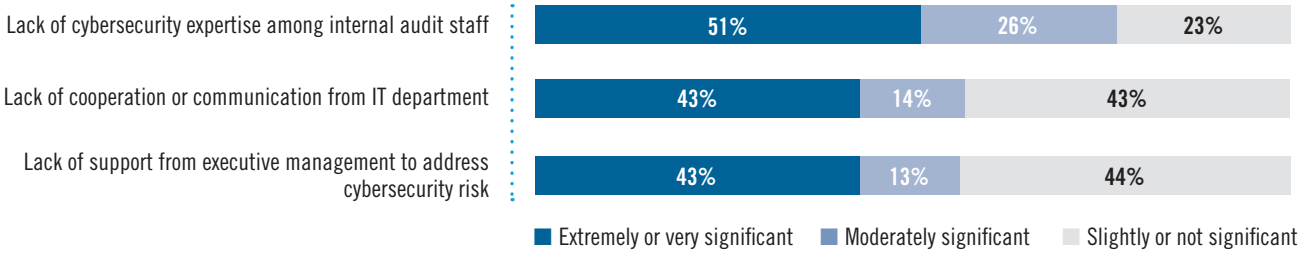
Internal Audit Continues to Struggle With Cyber

Despite organizations uniformly identifying cybersecurity and cyber awareness as key risk priorities, CAEs have significant concerns about cyber and IT risk to their organizations. Nearly 7 in 10 (68 percent) rated the risk as high or very high for cyber and more than half (53 percent) rated the risk as high or very high for IT.[4] Every CAE should pause to ask themselves how often they discuss with the audit committee these concerns and whether internal audit has the ability/resources to deal with these issues.

Contributing to the high risk rating is internal audit's continued struggle to strengthen its skills in this significant risk area. More than half of CAEs identified a lack of cybersecurity expertise among internal audit staff as having an extremely or very significant effect on internal audit's ability to address cybersecurity risks. Further, more than 4 in 10 CAEs identified a lack of cooperation or communication from IT and a lack of support from executive management as having an extremely or very significant effect (Exhibit 4).

CAEs clearly understand the risk that cyber and IT issues present to their organizations. However, survey responses also make clear that internal audit is making slow progress in hiring, availing itself of third-party expertise, or training staff who can provide consistent and valuable independent assurance in that risk area. The growing pace and sophistication of cyberattacks make this gap particularly troubling. These issues must be discussed with the audit committee, including candid dialogue about resources needed to achieve adequate assurance over IT and cyber.

Exhibit 4: Obstacles to Addressing Cybersecurity Risk



Note: Q8: How significant of an effect do each of the following obstacles have on internal audit's ability to address cybersecurity risk? $n = 503$ to 507.

Action Items

1. CAEs should report to the audit committee any progress — or lack thereof — in building cyber skills within the function and the reasons why. Candid discussions with the audit committee about where audit coverage is either inadequate or skill sets are lacking is the only way to prompt changes in those conditions.

2. CAEs should alert the audit committee and management of any cybersecurity effort gaps. This means CAEs must document the reasons effort gaps exist including insufficient resources for cosourcing or outsourcing, misaligned audit plan priorities, and any real or perceived disconnect with IT.

3. CAEs must invest more time in building relationships/partnerships with CISOs and CIOs. Lack of cooperation from IT may reflect a weak relationship or concerns about internal audit's lack of cyber competence.

4. CAEs must invest more time in educating their teams about cybersecurity, including developing an in-depth understanding of the frameworks commonly used in cybersecurity such as NIST CSF, NIST 800-53, ISO/IEC 27001.

5. CAEs must consider cosourcing as a viable option, when in-house skills are not adequate.

6. CAEs should look for opportunities for their staffs to perform basic cybersecurity auditing with support from IT that does not require cyber expertise, such as identifying the organization's most significant assets in need of protection, testing insider threat controls and evaluating processes and structures designed to protect against accidental or inadvertent disclosure of organization information.

Resources

- Artificial Intelligence: The Data Below (Internal Audit Foundation)
- Approaches to Upskilling for Internal Auditors (IIA Global Knowledge Brief)
- The Future of Cybersecurity in Internal Audit (Internal Audit Foundation and Crowe)
- Auditing Cyber Security: Evaluating Risk and Auditing Controls (ISACA)
- Cybersecurity Framework (National Institute of Standards and Technology {NIST})
- Global Information Security Survey (EY)
- ISO/IEC 27001:2013: Information Security Management Systems — Requirements (International Organization for Standardization/International Electrotechnical Commission {ISO/IEC})
- Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Rev. 4)

Key Takeaways

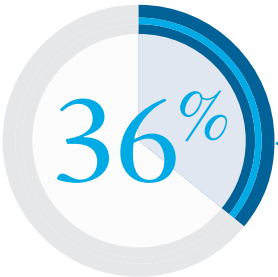
Reputational damage related to cyber breaches remains a top organizational concern for North American CAEs.

of CAEs say their organizations have high or very high **concerns about potential reputational harm** caused by inappropriate disclosure of private data.

Internal audit lags in developing the skills and expertise to provide assurance on cyber.

of CAEs cite **lack of cyber expertise** on staff as an obstacle to addressing cyberscurity risk.

There is an effort gap between the level of effort currently exerted by internal audit functions on key cyber areas and the level that CAEs believe they should be exerting.



CAEs report a 36% **gap between actual vs. desired assurance** over readiness and response to cyber threats.

The effort gap may reflect that internal audit is failing to adapt quickly enough to changing risks and stakeholder needs, and that potential misalignment exists between risks and audit plan priorities.

SECTION 2

Third-party Risks

The Pulse survey collected valuable data regarding CAEs' views on how their organizations handle third-party risks. The data reflect that organizations rely heavily on third-party providers in the key risk areas, including IT and business services. According to CAEs, 8 in 10 organizations have third-party contracts for IT services and 7 in 10 have them for other business services such as supply chain or accounting.[5]

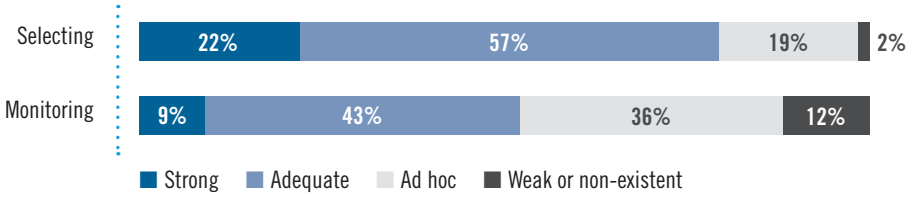
CAE responses clearly indicate there is significant concern about how third parties are selected and monitored, and how prepared organizations are for managing poorly performing vendors.

of CAEs consider their organization's **third-party selection processes** ad hoc, weak, or non-existent.

Selection, Monitoring Processes Cause Alarm

Nearly as many CAEs surveyed describe their organizations' third-party selection processes as ad hoc, weak, or non-existent — 21 percent — as those who describe them as strong — 22 percent. The remainder — 57 percent — describe the process as adequate. Similarly troubling numbers are reflected for organizations' monitoring of third-party providers, where only 9 percent of CAEs describe the oversight as strong while 43 percent say they are adequate and 48 percent describe them as ad hoc, weak, or non-existent (Exhibit 5).

Exhibit 5: Organizational Effort When Selecting and Monitoring Third-party Service Providers

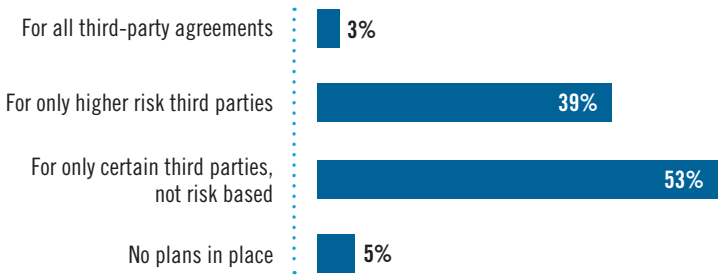


Note: Q28 and Q29: How would you describe your organization's efforts to "select" (Q28) and "monitor" (Q29) third-party service providers? $n = 498$.

Recovery Plans a Rare Luxury

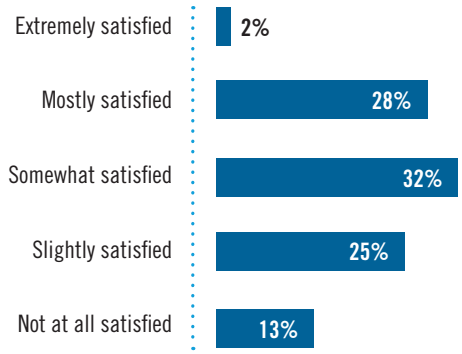
The frequency of recovery plans designed to address poor performance by a third-party service provider also is an area of concern. Recovery plans are designed to protect organizations by identifying a process for terminating contracts that minimizes disruption of services, limits legal liabilities, and protects the organizational assets and reputation. Yet more than half of CAEs reported that their organizations create such recovery plans on an ad hoc basis. Overall, only 42 percent of CAEs described their organizations as having recovery plans in place for all third-party agreements or those that present higher risks to the organization (Exhibit 6). Fewer than one-third of CAEs (30 percent) describe their overall satisfaction with their organizations' third-party risk management as extremely or mostly satisfied (Exhibit 7).

Exhibit 6: Frequency of Recovery Plans to Address Poor Performance of Third Parties



Note: Q30: To what extent does your organization have recovery plans to address poor performance of a third-party service provider? $n = 463$.

Exhibit 7: Satisfaction With Organization's Third-party Risk Management



Note: Q31: In general, how satisfied are you with your organization's management of risk related to third-party vendors? $n = 496$.

Third-party Assurance and the Ecosystem of Risk

Despite the significant concerns expressed by CAEs, survey responses reflect minimal audit plan allocation for examining third-party relationships. The average audit function allocates about 4 percent of its resources to third-party risk assurance, a trend that dates back to 2013, according to Pulse survey data. The frequency of cyberattacks facilitated by third-party vulnerabilities alone should prompt a re-examination of where this risk should rate as an audit plan priority. Eight high-profile organizations experienced significant breaches due to third-party exposures in the first half of 2018 alone, as noted by cybersecurity consultant Cyber GRX. Hackers exploited weaknesses in point of sale systems, chat and customer service platforms, and workflow automation and scheduling systems that conservatively exposed more than 250 million customer records.[6] New data privacy and protection rules in Europe, the U.S., and China introduce further compliance and financial risks.

Third-party risks aren't limited to cyber. Third-party relationships carry potential fraud and corruption, operational, and reputation risks, as well. Organizations cannot afford to view risks related to third-party relationships as separate from the organization's own risk landscape. All risks — direct, secondary, tertiary, and beyond — are part of the ecosystem of risk in which the organization operates. Just as organizations have come to understand supply chain risks can be impacted by seemingly unrelated events on the other side of the globe, so too must they understand that control weaknesses can be inherited through third-party relationships.

Action Items

1. CAEs must make the audit committee aware of any deficiency in third-party selection, monitoring, and recovery plan processes.
2. CAEs should proactively identify all the third-party relationships and risk rate them with relationship owners based on size, complexity, and impact to the organization.
3. CAEs should determine with each relationship owner — possibly through surveys — the key controls, oversight, and audits currently in place and inform the audit committee of the results.
4. CAEs should determine which relationships merit audits and conduct the audits.

Resources

- Auditing Third-party Risk Management (IIA Practice Guide)
- Auditing Outsourced Functions: Risk Management in an Outsourced World (Internal Audit Foundation)
- Oversight of Third-party Risks: Insights From the Audit Committee Leadership Networks (EY)

Key Takeaways

More than half of CAEs report that recovery plans to address poorly performing vendors are created without consideration of risk.

of CAEs report **recovery plans** are created for certain third-party relationships, but are not based on risk.

Few CAEs are satisfied with their organizations' management of third-party vendor risk.

of CAEs say they are extremely or mostly satisfied with their organization's **third-party risk management.**

CAEs must elevate the discussion to ensure management and the board understand that third-party relationships contribute to the overall ecosystem of risks and are not separate from the organization.


INTERNET

SECTION 3

Emerging and Atypical Risks

Dynamic geopolitical environments, shifting global economic conditions, and disruptive technology have brought emerging and atypical risks to the forefront of boardroom and C-suite discussions. New technologies and business concepts, from artificial intelligence to cryptocurrencies to 5G mobile connectivity promise to rewrite the rules on unconventional risks as well as their potential to significantly impact organizations.

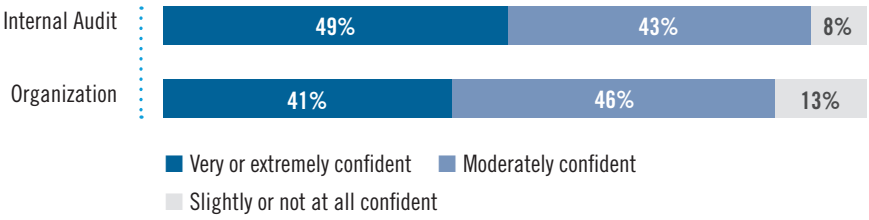
Like never before, alignment and collaboration among all risk functions is vital as organizations identify, decipher, and assess emerging and atypical risks.

Responses to the Pulse survey suggest CAEs are largely confident in the ability of their organizations and internal audit functions to identify and assess emerging risks, with 92 percent of CAEs saying they are very, extremely, or moderately confident (Exhibit 8). Emerging risks are defined for the purposes of the survey as "new risks or those that were of no consequence in the past."

The confidence drops only slightly when identifying atypical risks, described as "risks that are difficult to define and assess, or those very infrequent in occurrence." Eight in 10 CAEs say they are very, extremely, or moderately confident about their audit function's ability to identify and assess atypical risk. Their confidence dips slightly to 7 in 10 in describing their organization's ability to identify and assess atypical risk (Exhibit 9).

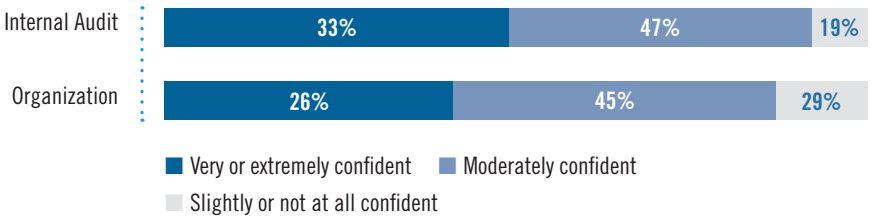
Only 3 in 10 CAEs report they use **advanced data analytics** to identify and assess emerging and atypical risks.

Exhibit 8: Confidence in Identifying and Assessing Emerging Risks*



Note: Q18: Please rate your confidence in the abilities of your organization and internal audit to identify and assess emerging risks. *Emerging risks are new risks or those that were of no consequence in the past. $n = 509$.

Exhibit 9: Confidence in Identifying and Assessing Atypical Risks*

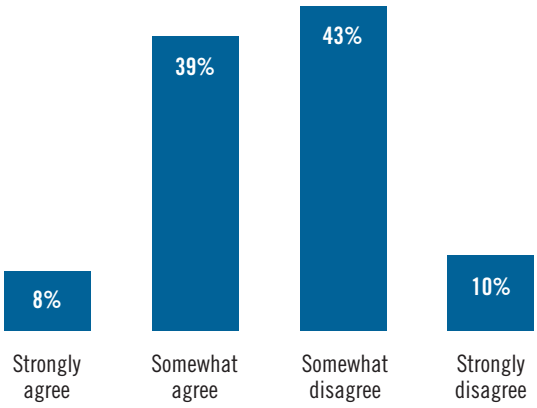


Note: Q19: Please rate your confidence in the abilities of your organization and internal audit to identify and assess atypical risks. *Atypical risks were defined in the survey as risks that are difficult to define and assess, or those very infrequent in occurrence $n = 509$.

Surprises Belie Confidence

However, this confidence is somewhat contradicted by CAE responses to two follow-up questions. First, 47 percent of CAEs strongly agreed or somewhat agreed with the statement, "It is fairly common that an emerging or atypical risk will surprise management" (Exhibit 10). Second, 24 percent reported a "surprise risk" in the previous 12 months.[7]

Exhibit 10: It Is Fairly Common* That an Emerging or Atypical Risk Will Surprise Management

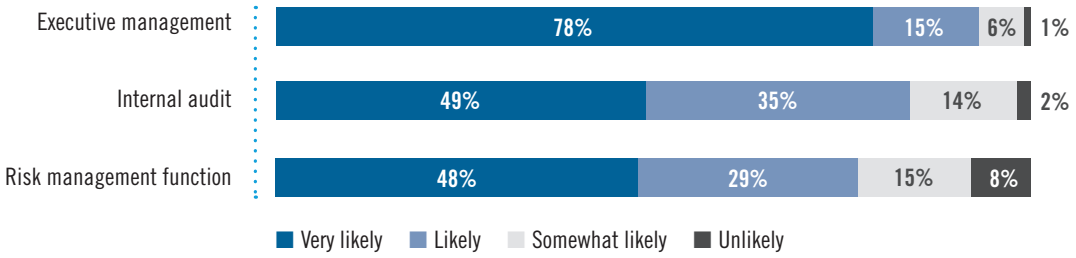


Note: Q24: Please rate your level of agreement with the following statement: It is fairly common that an emerging or atypical risk will surprise management.* "Fairly common" was described in the survey as "more than once a year there is a risk requiring the attention of executive management that was not foreseen." $n = 500$.

Internal Audit Involvement Marginal

This incongruity can be further explored by looking at the sources that the board relies upon for information about emerging or atypical risks. Internal audit is not normally where boards turn for identification of emerging or atypical risks. About three-quarters of CAEs rated the board as very likely to rely on executive management, but fewer than half said the same for internal audit or the risk management function (Exhibit 11).

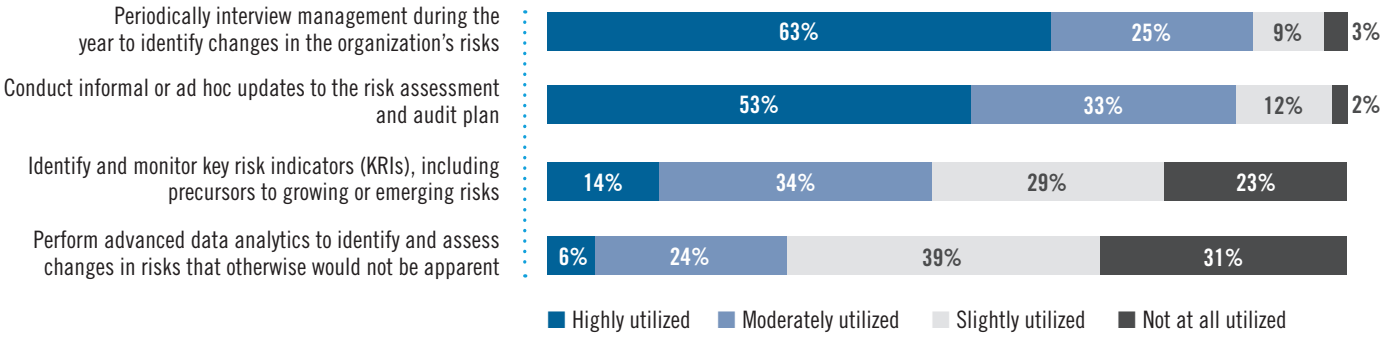
Exhibit 11: Board Reliance on Various Parties to Identify and Assess Emerging or Atypical Risks



Note: Q23: Please rate the likelihood that the board (or similar) relies on the following parties in identifying and assessing emerging or atypical risks. Those who chose "not applicable" were not included in the analysis for that variable. *n* = 418 to 503.

It is troubling that responses from CAEs may reflect a misplaced confidence in the ability of their organizations to identify and mitigate emerging or atypical risks. For example, while most CAEs reported management interviews and formal periodic updates of the risk assessment and audit plans as highly or moderately used methods to assess risks, fewer than half identify and monitor key risk indicators (KRIs), including precursors to growing or emerging risks (Exhibit 12). This places greater reliance on what the board hears from management than what it can independently determine from objective measures such as KRIs. It also may shed some light on the difference between the CAE confidence levels and the frequency of reported surprise risks.

Exhibit 12: Use of Risk Assessment Methods



Note: Q20: Please indicate the degree to which internal audit at your organization uses the following methods to assess risk. *n* = 504 to 511.

Action Items

1. CAEs should proactively monitor and keep up to date on:
   - Economic forecasts.
   - New initiatives being planned.
   - Legislative and regulatory outlooks.
   - Threats and opportunities facing the industry.
   - Primary competitors and their challenges.
   - Risks emerging in headlines via traditional or social media.

2. CAEs should address with management and the board/audit committee expanding internal audit's role in identifying and assessing emerging or atypical risks.

3. CAEs should challenge risk management practices that rely solely on management interviews about what is being done to monitor emerging and atypical risks rather than asking how and why it is being done.

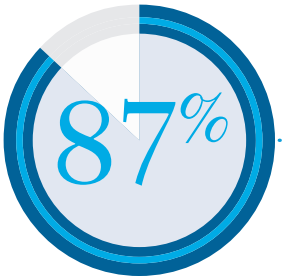
4. CAEs should focus on improving how their organizations use KRIs, data analytics, and other tools to identify and monitor precursors to growing and emerging risks.

Resources

- Internal Audit and Emerging Risks: From Hilltops to Desktops (Chambers on the Profession)
- Auditing and Disruptive Technologies (Internal Audit Foundation)
- International Risk Governance Council (Website)

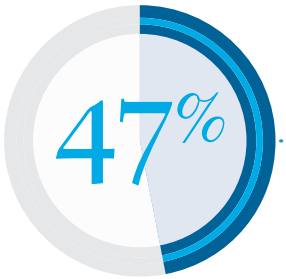
Key Takeaways

CAEs are highly confident in the ability of their organizations and audit functions to identify and assess emerging and atypical risks.



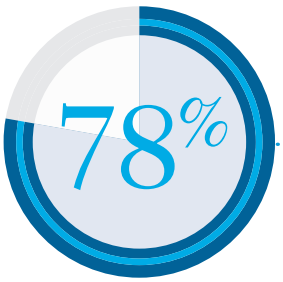
of CAEs are extremely or moderately confident in their organization's **ability to identify and assess emerging risks.**

Nearly half of CAEs said management is frequently surprised by an emerging or atypical risk.



of CAEs say it is fairly common that an **emerging or atypical risk will surprise management.**

CAEs report internal audit is not at the top of the board's list for information on emerging and atypical risks.



of CAEs say the board will turn to management for **identification and assessment of emerging and atypical risks.**

CAEs report the board is much more likely to turn to management for identification and assessment of emerging and atypical risks.

SECTION 4

Board and Management Activity

Regulatory pressures, especially in the areas of financial reporting and cybersecurity, are growing, placing board and management oversight in the spotlight. Recent governance and data protection failures in banking and social media platforms have led to top executives being called before congressional committees to explain their actions and some board members being forced to resign.

Boards are more carefully scrutinizing the information they receive from management. For example, board members report they spend nearly twice as much time reviewing materials from management as they allocate to reviewing relevant information from external sources, according to the 2018–2019 NACD Public Company Governance Survey. What's more, "Fifty-three percent of directors indicate that the quality of management reporting to the board must improve, suggesting boards need better — not more — information from management," according to the findings.[8]

The 2019 Pulse survey sought to gauge, from the CAE perspective, whether boards are getting a complete picture on risks and whether internal audit has a role in providing assurance on the information that boards receive.

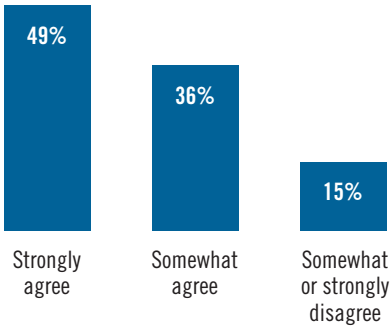
of board directors responding to an NACD survey said the **quality of management reporting must improve.**

Informing the Board

Generally, CAEs believe boards get the information they need in vital areas of risks. The overwhelming majority strongly or somewhat agree that the information management provides to the board regarding potentially significant risks is accurate, ongoing, complete, representative, timely, and transparent. For example, responses from CAEs find that 85 percent strongly or somewhat agree that all pertinent information gets to the board, rather just the information that supports management's views (Exhibit 13).

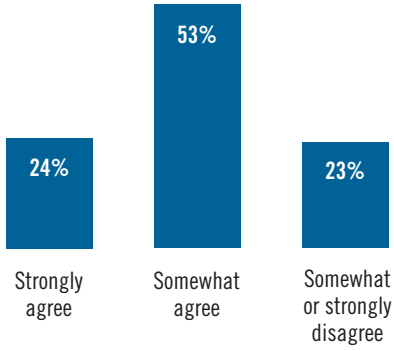
However, one area of potential concern involves the influence of short-term considerations on information going to the board from management. While 24 percent of CAEs strongly agree management primarily evaluates issues based on long-term impact to the organization, and 53 percent somewhat agree, nearly one-quarter — 23 percent — somewhat or strongly disagree (Exhibit 14).

Exhibit 13: Management Provides the Board With All Pertinent Risk Information



Note: Q11: Indicate your level of agreement or disagreement about characteristics of information management provides to the board (or similar). Topic: Complete — all pertinent information is provided, not just that supportive of the views of management. *n* = 495.

Exhibit 14: Management Evaluates Issues Based on Long-term Impact



Note: Q10: Indicate your level of agreement or disagreement with each of the following statements regarding the current state of your organization. Topic: Management primarily evaluates issues based on long-term impact to the organization. *n* = 495.

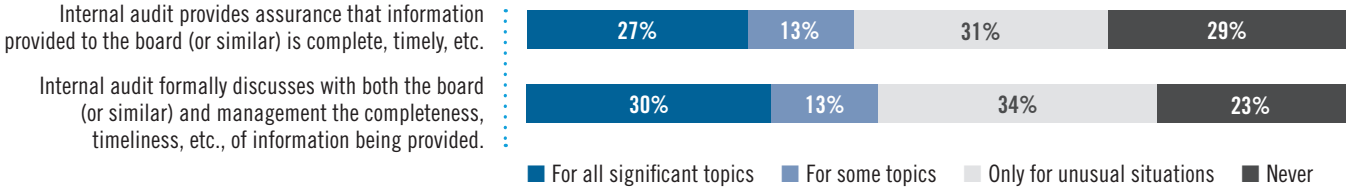
Internal Audit's Peripheral Involvement

The data paint a less encouraging picture about how often internal audit provides assurance on the information that goes to the board. Nearly 6 in 10 CAEs report that internal audit rarely or never provides assurance on the quality of information given to the board nor does internal audit have formal discussions about the information with the board and management (Exhibit 15).

Another important consideration is that boards often have multiple committees that do not involve internal audit or the CAE (e.g. compensation committee, risk committee, IT committee). Internal audit has limited ability to evaluate and provide assurance on the quality of information the board receives from these committees.

As regulators' expectations grow about board oversight, internal audit may be asked more often to provide assurance on information the board receives. CAEs should examine and fully understand the processes involved in getting information to the board and be prepared to audit any information about which the board seeks independent assurance. They can begin by auditing any related controls, if they exist, or alerting the board to the lack of such controls. Ultimately, the goal is to make the board aware that, while rarely asked, internal audit can provide assurance or advisory services on information the board receives.

Exhibit 15: Internal Audit Activity Related to Information Board Receives From Management



Note: Q13: Indicate the nature of internal audit's engagement with the information provided by management to the board (or similar) on significant topics. *n* = 473.

Getting Internal Audit's Voice Heard

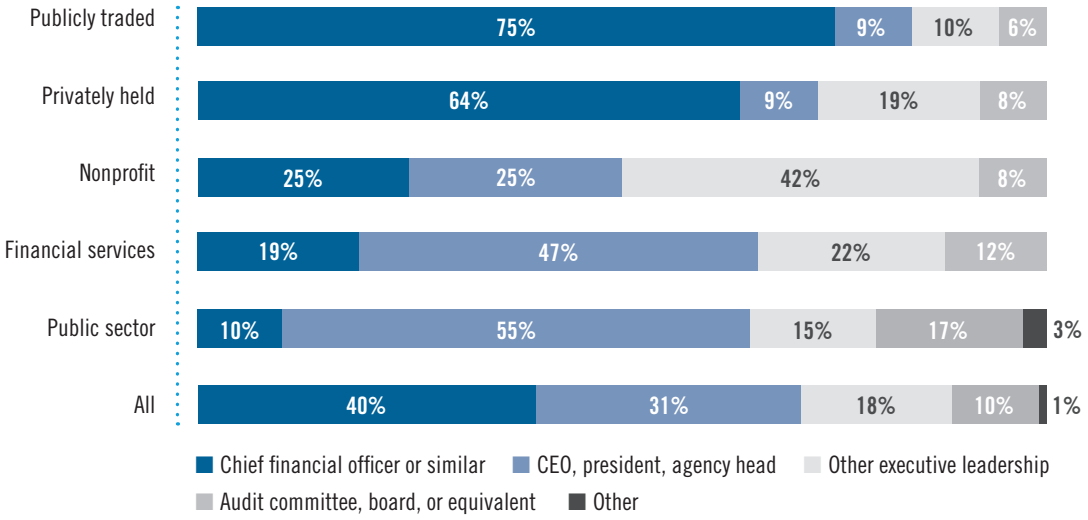
Analysis of CAE responses about the board and management activities indirectly raises a fundamental question of whether traditional reporting lines are sufficient to ensure that internal audit findings and recommendations are being heard. The IIA supports a dual reporting line structure where internal audit reports administratively to the CEO and functionally to the board.[9] In practice, most organizations have functional reporting lines where the CAE reports to the audit committee of the board.

However, variances in audit committee structure and responsibility — as noted earlier — create the real possibility that in some organizations internal audit is not involved with committees that handle critical issues, such as cybersecurity and overall risk governance. For example, in many organizations, risk and IT committees, not audit committees, are tasked with overseeing cybersecurity and cyber preparedness. Such conditions could handicap internal audit's ability to deliver perspectives about those vital risk domains.

Additionally, the administrative reporting line in many organizations could further limit internal audit's ability to communicate with the CEO. For example, many organizations continue to have the CAE report administratively to the chief financial officer, which creates an additional reporting layer between the CAE and the CEO.

Among Pulse survey respondents overall, 4 in 10 say they report administratively to the CFO while 3 in 10 report to the CEO, with the remainder reporting elsewhere within the organization. A breakdown by type of organization shows that CAEs in publicly traded and privately held organizations are much more likely to report to the CFO – about 7 in 10 (Exhibit 16).

Exhibit 16: Administrative Reporting Lines*



Note: Q34: What is the primary administrative* reporting line for the chief audit executive (CAE) or head of internal audit in your organization? *Administrative reporting refers to oversight of day-to-day matters, expense approval, human resource administration, communication, internal policies and procedures. $n = 505$.

Action Items

1. CAEs should proactively discuss with the audit committee chair internal audit's willingness to provide assurance on the accuracy, completeness, timeliness, transparency, and reliability of data provided to the board.

2. CAE should ask to be copied on material going to the board and at a minimum provide negative assurance on its accuracy, completeness, timeliness, transparency, and reliability. In the instance, negative assurance would be defined as internal audit affirming the accuracy, completeness, timeliness, transparency, and reliability of material going to the board when no contrary evidence is found.

3. CAEs should ask to be present during other committee meetings, such as IT, risk, and compensation, where internal audit may share information and insights that are relevant to the board.

4. CAEs should share available research with the audit committee chair regarding preferred reporting lines for providing effective independent and objective assurance.

Resources

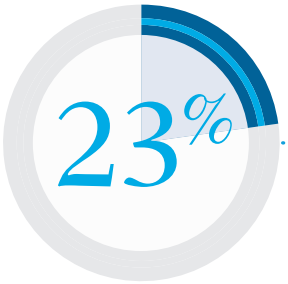
- The Audit Committee and the CAE: Sustaining a Strategic Partnership (Internal Audit Foundation)
- CAE Strategic Relationships: Building Rapport With The Executive Suite (Internal Audit Foundation)
- Interaction With the Board (IIA Practice Guide)
- Internal Auditing's Role in Corporate Governance (IIA Position Paper)
- Why Conformance Matters (IIA Position Paper)

Key Takeaways

Generally, CAEs believe executive management gives boards the risk information that the boards need.

of CAEs agree that all **pertinent information gets to the board,** rather than just what supports management's view.

However, management may not always take the long view.



of CAEs say executive management does not look at **the long-term impact of issues.**

Internal audit is rarely asked to provide assurance on information going to the board.

of CAEs report they **rarely or never discuss with the board or management** the accuracy, completeness, timeliness, truthfulness, and transparency of information going to the board.

Because internal audit typically reports to the audit committee, it may not have adequate involvement with other board committees that handle critical issues, such as IT or risk governance.

Conclusion

Internal audit is in a race to define its place in a rapidly changing world.

It is a place where the promise of a fourth industrial revolution — where connectivity and data are married seamlessly with technological breakthroughs in robotics and artificial intelligence — presents a powerful and enticing picture to the women and men who lead our organizations. Those who can master these world-changing developments will guide their organizations to success.

However, success will come only to those who can balance the opportunities and risks created by these technological advances, and internal audit must play a central role in helping them find that balance. This will require internal audit to develop team members with the necessary skills to provide independent assurance on increasingly complex risk issues and for its leaders to have the fortitude to make their voices heard in boardrooms and C-suites.

The 2019 North American Pulse of Internal Audit identifies four risk areas where internal audit can make its voice heard:

Cybersecurity

Internal audit must improve its efforts to provide high-level assurance and advisory services in this area. This requires building strong relationships with CIOs and CISOs, and accelerating efforts to build cyber-savvy teams through training, new hires, or cosourcing. CAEs must speak up about having the audit plan allocations properly reflect the importance of cyber and IT assurance and discuss any areas where the CAE feels internal audit must strengthen itself in this vital area.

Third-party Risks

Third-party relationships are part of every organization's ecosystem of risks, and organizations that fail to properly address third-party risks are in peril. Internal audit must educate boards and executive management to the dangers of weak or non-existent controls over third-party relationships and work closely with the audit committee and management to define the role that internal audit should play to provide assurance in this important area.

Emerging and Atypical Risks

Threats from emerging and atypical risks are growing as technology accelerates the speed at which they can mature and do damage to organizations. CAEs must educate themselves about emerging and atypical risks that can potentially impact the organization. CAEs must speak up when the organization relies solely on management assurances about mitigation of emerging and atypical risks. CAEs should push for stronger KRIs to monitor precursor indicators, and provide assurance on processes to identify, monitor, and mitigate emerging and atypical risks.

Board and Management Activity

Like never before, regulators and shareholders are pressing boards to provide proper governance oversight. They can best accomplish this if the information on which they base their decisions is accurate and complete. CAEs should position their functions to provide assurance on all information going to the board and educate the board and executive management about the benefits that independent assurance can provide.

For more than 75 years, internal auditors have shown great skill in pivoting to meet new challenges. The challenges they face today — complex, accelerated, global — will require agility, innovation, and effective dialogue with the board and executive management. It will require a fundamental commitment to assure boards have information that is accurate, complete, timely, transparent, and reliable.

Simply, for internal audit to find its place in this brave new world, practitioners must courageously raise their voices.

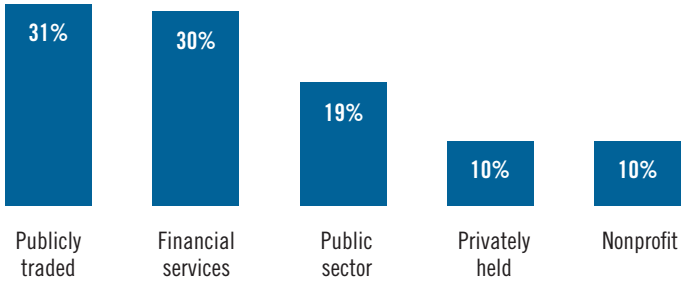
Appendix:

Internal Audit Management Metrics

CAEs need to have strong management skills — and the ability to efficiently use resources — to achieve the internal audit function's objectives. In the annual Pulse of Internal Audit survey, The IIA collects information on key internal audit management metrics, some of which will be provided in this section. More detailed reports will be made available to members of the AEC at www.theiia.org/AEC.

Internal audit management metrics have been cross-tabulated into five organization types — publicly traded, privately held, public sector, nonprofit, and financial services (Exhibit A). The financial services category was created by extracting financial services respondents from the other four organization types. The most common industries represented in each category are:

Exhibit A: Organization Type With Financial Services Breakout



Note: Q80: For what type of organization do you currently work? $n = 157$ for publicly traded, 151 for financial services, 96 for public sector, 53 for privately held, 48 for nonprofit.

Publicly Traded

- Manufacturing (30%)
- Mining, quarrying, and oil and gas extraction (10%)
- Utilities (9%)
- Retail trade (6%)
- Health care and social assistance (6%)
- Information (e.g., publishing, broadcasting, data processing) (6%)
- Other services (except public administration) (6%)

Financial Services

Financial Services Types

- Financial institution (55%)
- Insurance (28%)
- Asset management (7%)
- Broker-dealer (3%)
- Other (7%)

Organization Types

- Publicly traded (45%)
- Privately held (32%)
- Nonprofit (13%)
- Public sector (10%)

Public Sector

- Public administration (40%)
- Educational services (28%)
- Utilities (8%)
- Health care and social assistance (5%)

Privately Held

- Manufacturing (25%)
- Health care and social assistance (13%)
- Professional, scientific, and technical services (11%)
- Other services (except public administration) (9%)
- Educational services (8%)

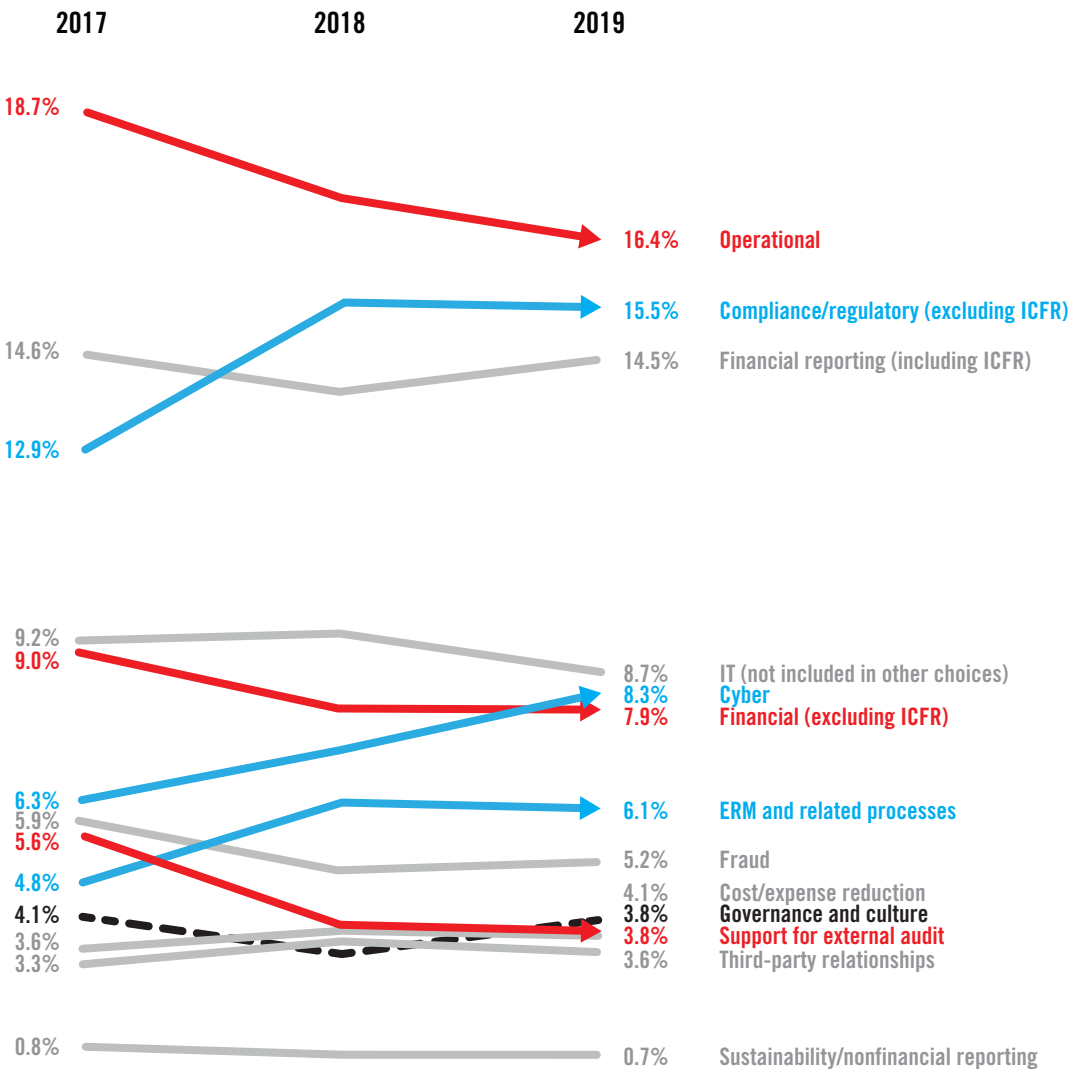
Nonprofit

- Health care and social assistance (58%)
- Educational services (15%)
- Other services (except public administration) (15%)

Audit Plan — All Respondents

The following section provides a breakdown of audit plans trends by category over a three-year period. The average of all respondents provides a good starting point and offers a big-picture perspective on audit plan efforts. But the most useful information comes from the breakdowns by organization type that follow. It should be noted that publicly traded and financial services each represent about one-third of the respondents and therefore drive the results of the overall average (Exhibit B).

Exhibit B: Audit Plan Allocation — All Respondents (2017 to 2019)



Note: Allocation of audit effort according to the annual Pulse survey from 2017 to 2019. ICFR = internal controls over financial reporting. The percentage allocated to "other" is not included in this graph. $n = 509$ in 2017, 636 in 2018, 512 in 2019.

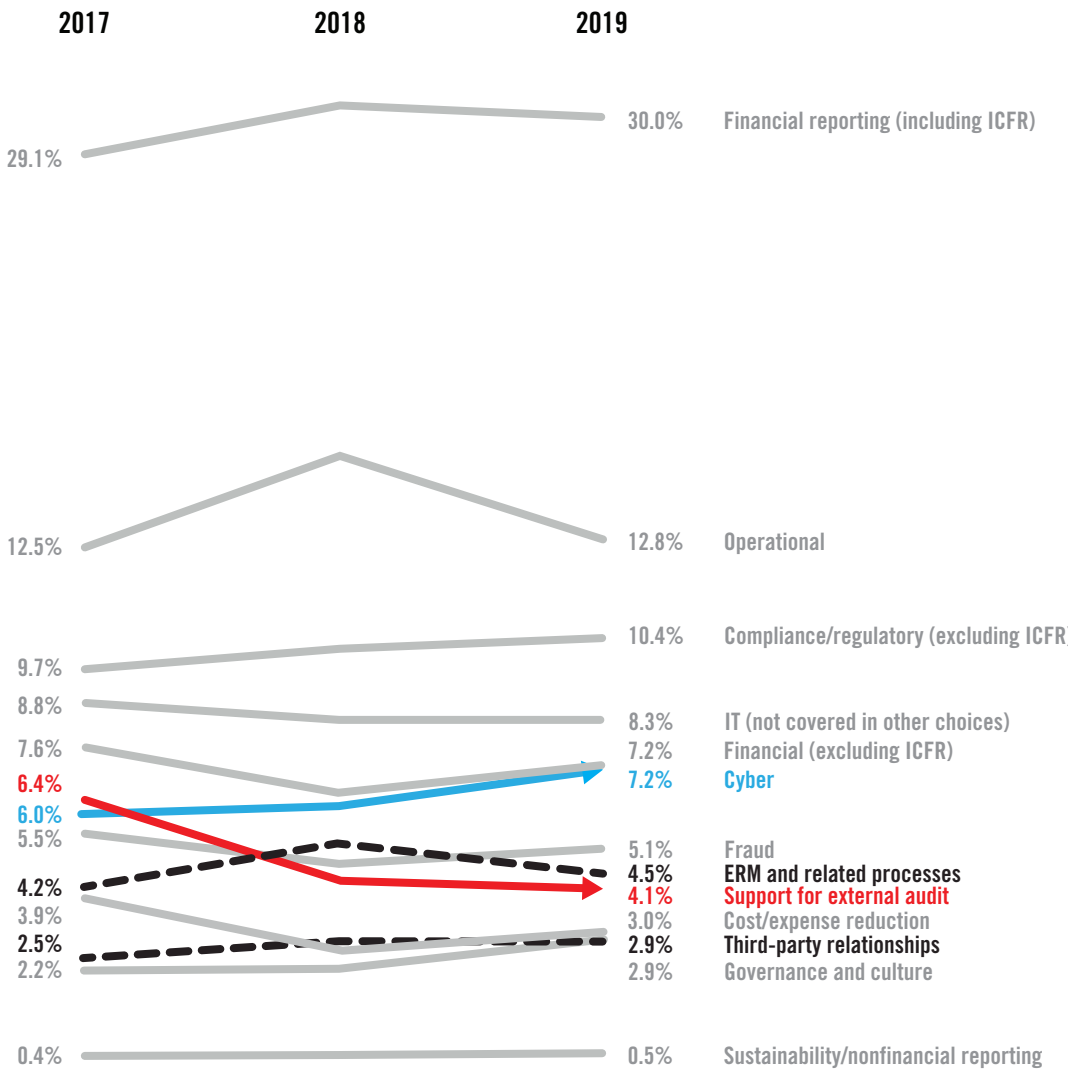
- Trending up (1 percentage point increase or more)
- Trending down (1 percentage point decrease or more)
- Neutral (solid line) (less than 1 percentage point change)
- Black (dashed line)* (less than 1 percentage point change)

*Dashed line is used to help with differentiating the lines.

Audit Plan — Publicly Traded

Financial reporting and compliance regulations clearly dominate efforts in audit functions in publicly traded companies. About 40 percent of audit plans in this type of organization are devoted to those two areas. When three other high-profile risk areas are added – operational, cyber, and IT – nearly 69 percent of the plan is devoted to five risk areas. This leaves the remaining 31 percent to be split among other significant risk areas including enterprise risk management, fraud detection and investigation, third-party relationships, and governance and culture (Exhibit C).

Exhibit C: Audit Plan Allocation — Publicly Traded (2017 to 2019)



Note: Allocation of audit effort according to the annual Pulse survey from 2017 to 2019. ICFR = internal controls over financial reporting. The percentage allocated to "other" is not included in this graph. Only publicly traded respondents (excluding financial services). *n* = 166 in 2017, 197 in 2018, 157 in 2019.

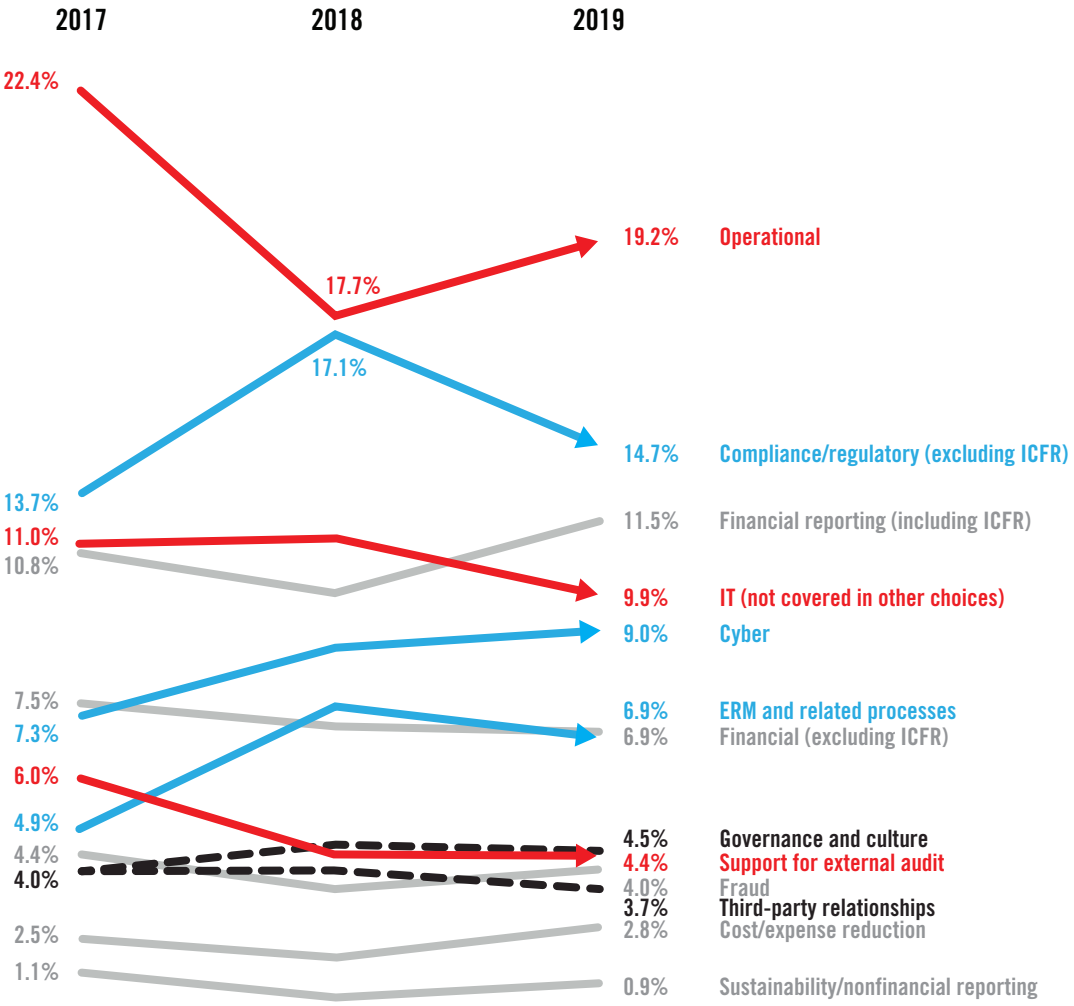
- Trending up (1 percentage point increase or more)
- Trending down (1 percentage point decrease or more)
- Neutral (solid line) (less than 1 percentage point change)
- Black (dashed line)* (less than 1 percentage point change)

*Dashed line is used to help with differentiating the lines.

Audit Plan — Financial Services

Despite the heavy regulatory environment in financial services, it is the only organization type where operational effort in audit plans exceeds compliance efforts. In comparison to publicly traded companies, financial services devotes only about a quarter of its audit plan (26 percent) to compliance and financial reporting (Sarbanes-Oxley). Indeed, financial services is able to devote a higher percent of the audit plan to operational, IT/cyber, ERM, third-party risk, and governance and culture risks than publicly traded organizations. It should be noted some organizations view compliance requirements, such as stress testing as part of operations, which could skew the operations allocation higher (Exhibit D).

Exhibit D: Audit Plan Allocation — Financial Services (2017 to 2019)



Note: Allocation of audit effort according to the annual Pulse survey from 2017 to 2019. ICFR = internal controls over financial reporting. The percentage allocated to "other" is not included in this graph. Only financial services respondents. $n = 139$ in 2017, 186 in 2018, 151 in 2019.

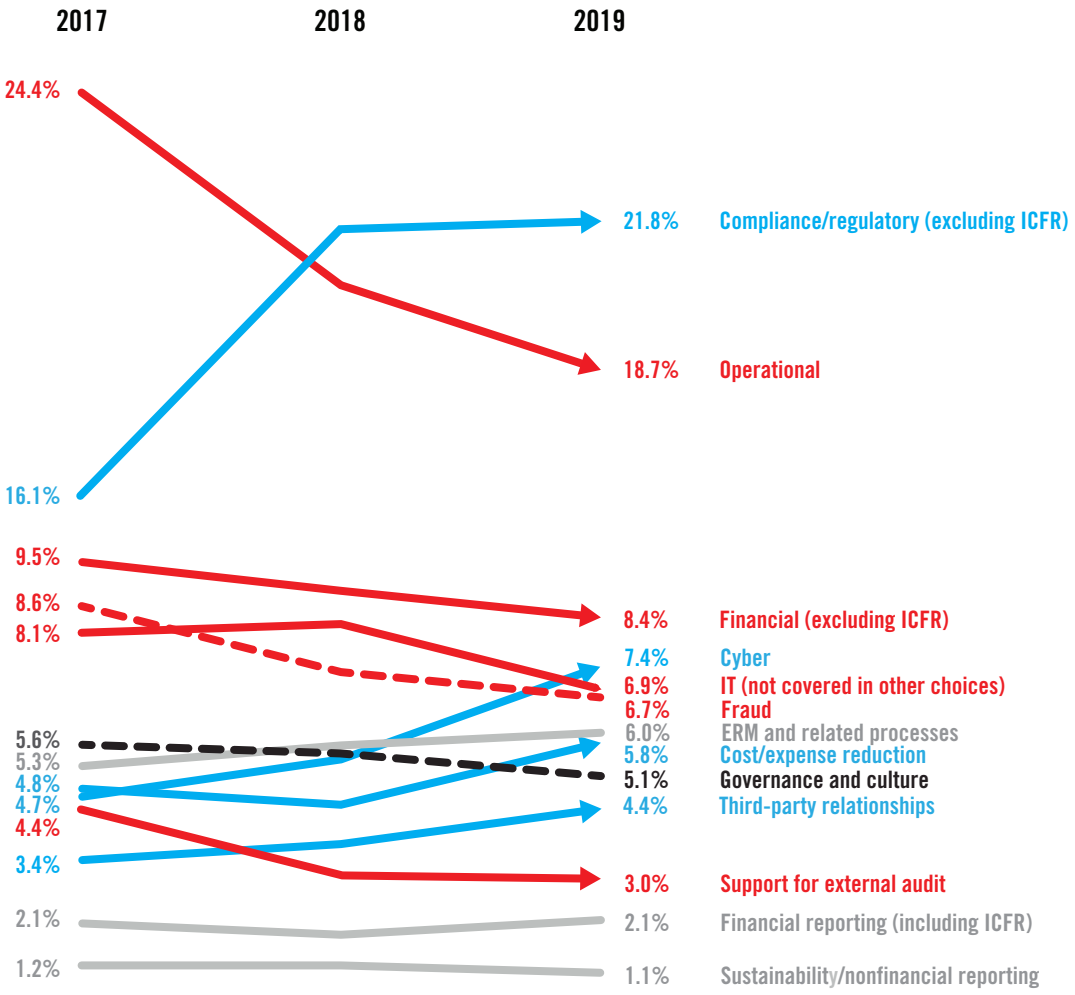
- Trending up (1 percentage point increase or more)
- Trending down (1 percentage point decrease or more)
- Neutral (solid line) (less than 1 percentage point change)
- Black (dashed line)* (less than 1 percentage point change)

*Dashed line is used to help with differentiating the lines.

Audit Plan — Public Sector

General compliance is the largest audit plan category for the public sector, which is driven largely by mandated compliance audits from legislatures or other governing bodies. Similarly, operational audits are driven by performance reviews of public agency economy, efficiency, and effectiveness use of available resources. While operational audit has dropped significantly as a percentage of the audit plan, it still rates as the second-highest priority. Public sector has a combined 14 percent for IT/cyber, which is only 1 percent lower than the average for all respondents (Exhibit E).

Exhibit E: Audit Plan Allocation — Public Sector (2017 to 2019)



Note: Allocation of audit effort according to the annual Pulse survey from 2017 to 2019. ICFR = internal controls over financial reporting. The percentage allocated to "other" is not included in this graph. Only public sector respondents (excluding financial services). $n = 103$ in 2017, 134 in 2018, 96 in 2019.

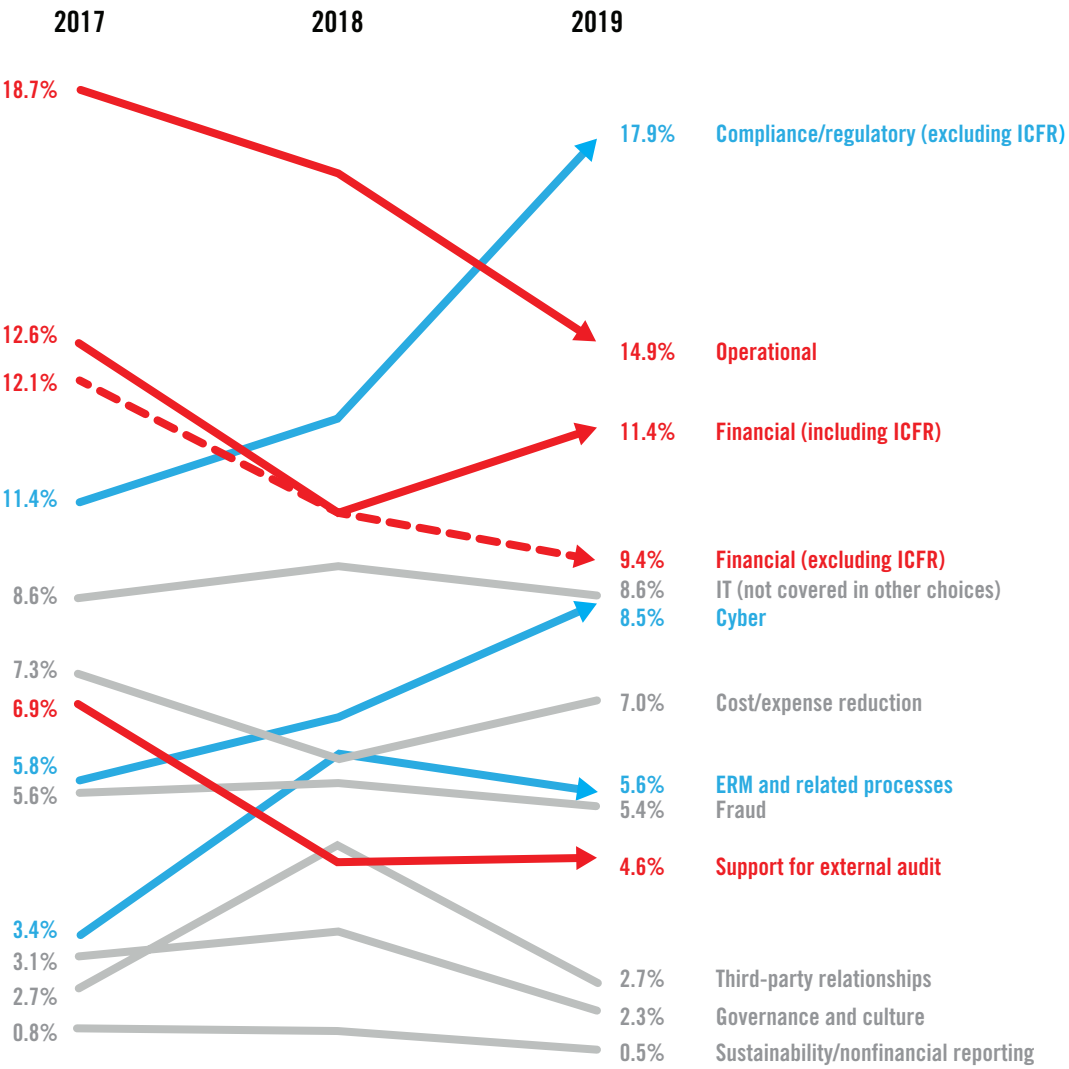
- Trending up (1 percentage point increase or more)
- Trending down (1 percentage point decrease or more)
- Neutral (solid line) (less than 1 percentage point change)
- Black (dashed line)* (less than 1 percentage point change)

*Dashed line is used to help with differentiating the lines.

Audit Plan — Privately Held

The privately held organization type is dominated by manufacturing, health care, and scientific services, which is reflected in the greater focus on non financial compliance and regulatory efforts. Risks for these industries are more likely to focus on environmental, health and safety concerns. The organization type also devotes a higher percent of effort to cyber and IT issues, which may reflect greater concerns about data protection, and which also can explain the sharp increase in compliance in 2018 when GDPR and other data protection and privacy rules went into effect (Exhibit F).

Exhibit F: Audit Plan Allocation — Privately Held (2017 to 2019)



Note: Allocation of audit effort according to the annual Pulse survey from 2017 to 2019. ICFR = internal controls over financial reporting. The percentage allocated to "other" is not included in this graph. Only privately held respondents (excluding financial services). $n = 50$ in 2017, 54 in 2018, 53 in 2019.

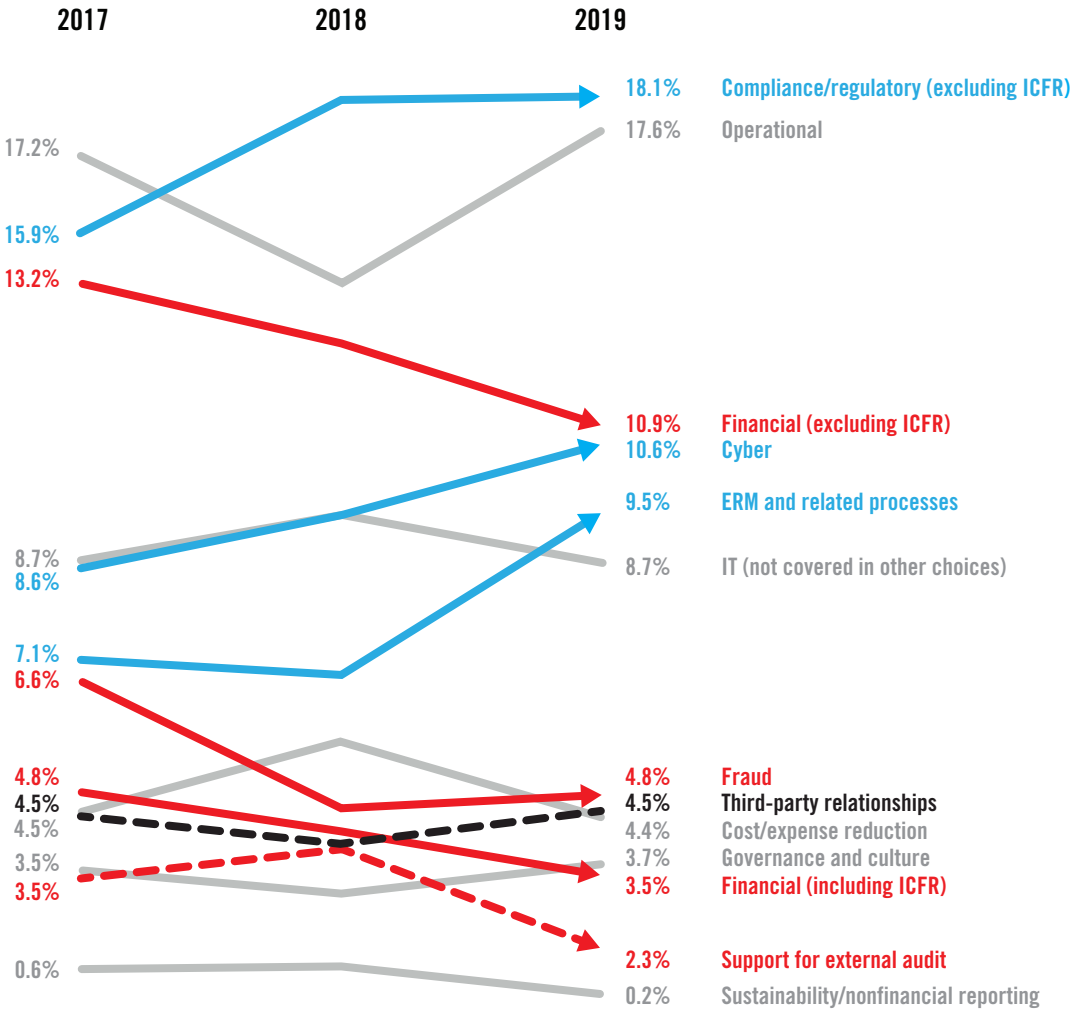
- Trending up (1 percentage point increase or more)
- Trending down (1 percentage point decrease or more)
- Neutral (solid line) (less than 1 percentage point change)
- Neutral (dashed line)* (less than 1 percentage point change)

*Dashed line is used to help with differentiating the lines.

Audit Plan — Nonprofit

It should be noted that responses for this organization type were primarily from health care and social assistance organizations (58 percent), which is reflected in the similar audit plan effort breakdown for privately held organizations. Indeed the two top risk areas are almost identical for both groups. Both groups also devote a higher percentage of their audit plans to IT/cyber than the average. Organizations in the non profit category devote the highest percentage of their audit plans to IT/cyber — 20 percent — compared to the overall average of 17 percent. They also devote the highest percentage to enterprise risk management — 10 percent — compared to the overall average of 6 percent (Exhibit G).

Exhibit G: Audit Plan Allocation — Nonprofit (2017 fo 2019)



Note: Allocation of audit effort according to the annual Pulse survey from 2017 to 2019. ICFR = Internal controls over financial reporting. The percentage allocated to "other" is not included in this graph. Only nonprofit respondents (excluding financial services). $n = 51$ in 2017, 54 in 2018, 48 in 2019.

- Trending up (1 percentage point increase or more)
- Trending down (1 percentage point decrease or more)
- Neutral (solid line) (less than 1 percentage point change)
- Black (dashed line)* (less than 1 percentage point change)

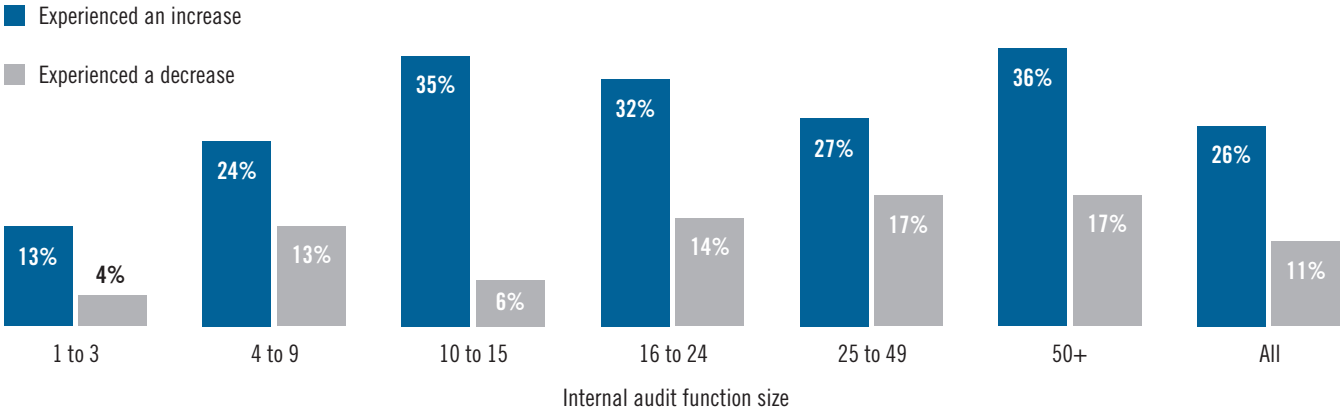
*Dashed line is used to help with differentiating the lines.

Staffing

For internal audit staff size last year, more than twice as many CAEs reported an increase versus a decrease (26 percent to 11 percent). It is worth noting that the smallest functions (1 to 3 FTEs) are significantly less likely to experience an increase compared to the overall average (13 percent compared to 26 percent). The most growth took place in functions with 10 to 15 FTEs, where 35 percent reported increases compared to only 6 percent with decreases (Exhibit H).

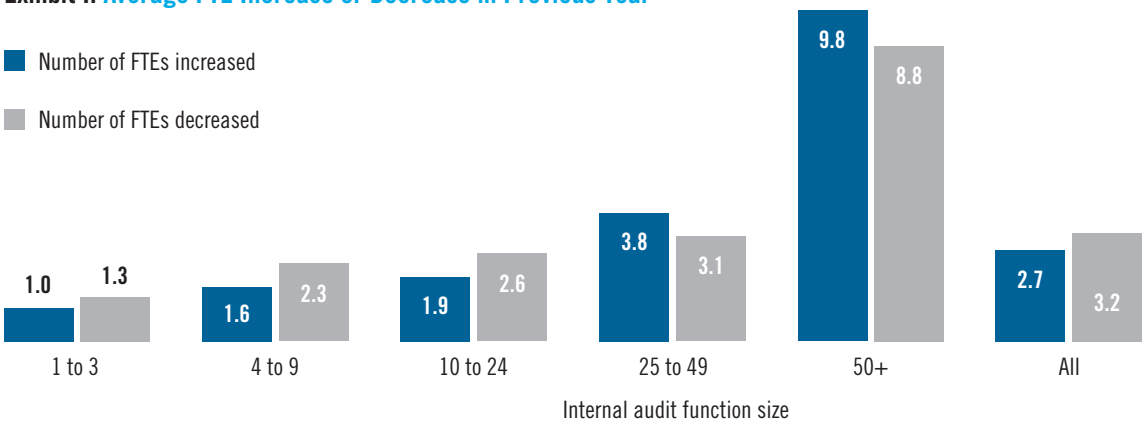
The graph at the bottom of the page shows the number of FTEs that were increased or decreased among those internal audit functions that experienced a change. Increases averaged 2.7 FTEs while decreases averaged 3.2 FTEs. It should be noted that functions with 50 or more FTEs reported greater volatility, with notably higher FTE increases and decreases (Exhibit I).

Exhibit H: Internal Audit Functions Reporting Increase or Decrease in Previous Year



Note: Q42: Looking back over the past 12 months, the number of full-time equivalent staff (employees, contractors, cosourced, and outsourced) within your internal audit function has: experienced an increase, remained the same, or experienced a decrease. FTE stands for full-time equivalent employee. *n* = 500.

Exhibit I: Average FTE Increase or Decrease in Previous Year

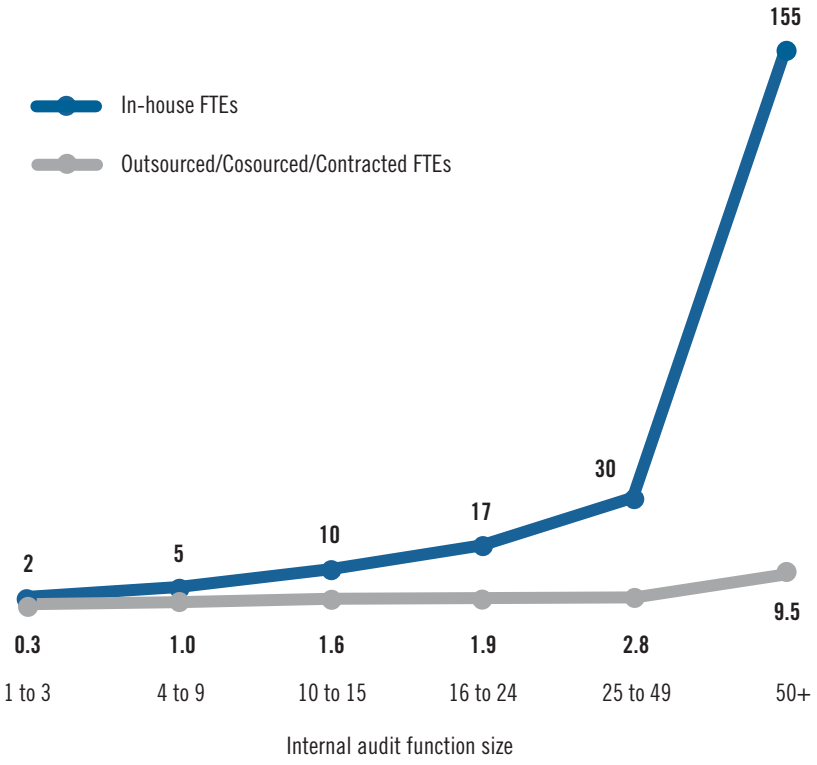


Note: Q43: By how many FTEs did your staff increase (employees, contractors, cosourced, and outsourced)? n = 129. Compared to Q44: By how many FTEs did your staff decrease (employees, contractors, cosourced, and outsourced)? FTE stands for full-time equivalent employee. *n* = 54.

In-house, Outsourced, Cosourced, and Contracted

For the first time, the Pulse management metrics includes data about the number of FTEs outsourced, cosourced, or contracted for internal audit activity. As shown in Exhibit J, the number of non-internal-audit FTEs generally ranges between 1 and 3 and does not increase proportionately with internal audit function size. This suggests the impact of outsourcing is greater for smaller functions.

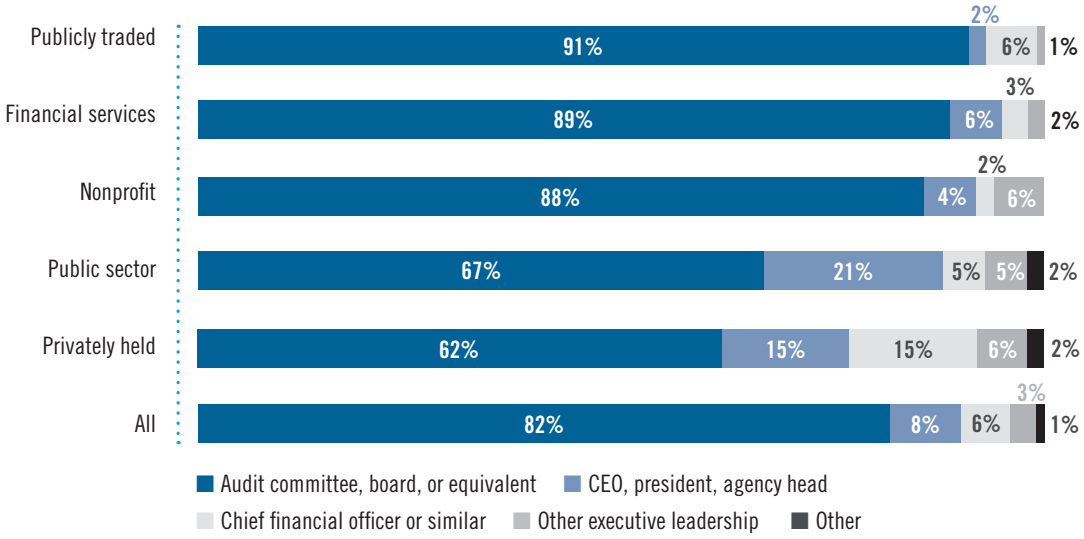
Exhibit J: Inhouse Internal Audit FTEs Compared to Outsourced/Cosourced/Contracted FTEs*



Note: Q37: Enter the approximate number of in-house FTEs (including the CAE, employees, and long-term contractors). Q38: Enter the approximate number of other FTEs obtained through short-term contracts, cosourcing, outsourcing, or other similar means. FTE stands for full-time equivalent employee. *Several very large internal audit functions in the 50+ category have caused the average FTEs for this group to be very high relative to other functions. $n = 502$.

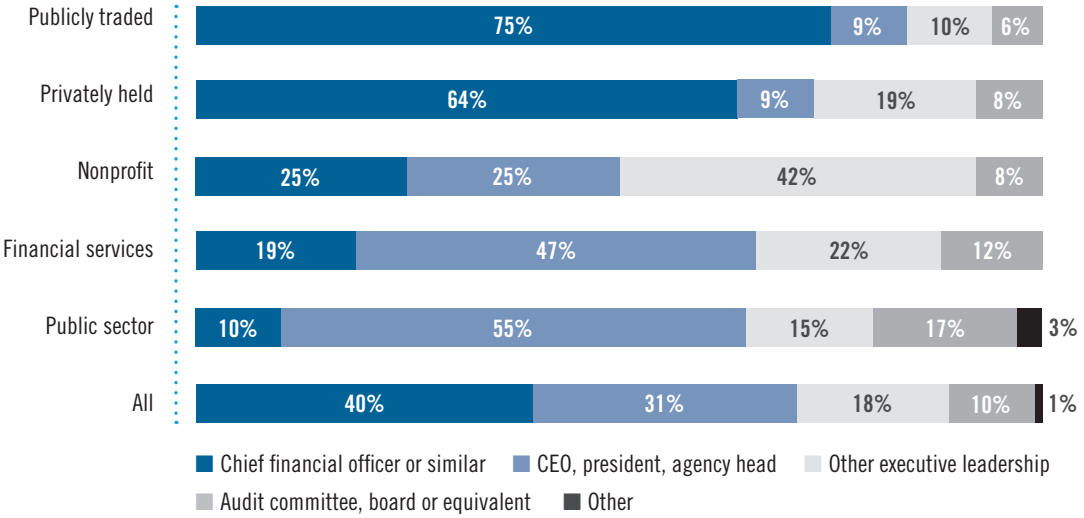
Reporting Lines

Exhibit K: Functional Reporting Lines*



Note: Q35: What is the primary functional* reporting line for the chief audit executive (CAE) or head of internal audit in your organization? *Functional reporting refers to the oversight of the responsibilities of the internal audit function, including approval of the internal audit charter, approval of the audit plan, evaluation of the CAE, compensation for the CAE. *n* = 505.

Exhibit L: Administrative Reporting Lines*



Note: Q34: What is the primary administrative* reporting line for the chief audit executive (CAE) or head of internal audit in your organization? *Administrative reporting refers to oversight of day-to-day matters, expense approval, human resource administration, communication, internal policies and procedures. *n* = 505.

Notes

1. 2018–2019 NACD Public Company Governance Survey: Key Findings (Arlington, VA: National Association of Corporate Directors, Dec. 2018), Key Finding 3, accessed at https://www.nacdonline.org/insights/publications.cfm?ItemNumber=63799.

2. 2018–2019 NACD Public Company Governance Survey: Key Findings (Arlington, VA: National Association of Corporate Directors, Dec. 2018), Key Finding 9, accessed at https://www.nacdonline.org/insights/publications.cfm?ItemNumber=63799.

3. 2018–2019 NACD Public Company Governance Survey: Key Findings (Arlington, VA: National Association of Corporate Directors, Dec. 2018), Key Finding 1, accessed at https://www.nacdonline.org/insights/publications.cfm?ItemNumber=63799.

4. Q52: How would you describe the level of risk in your organization in the following risk areas? $n = 502$.

5. Q27: Which types of third parties are significant in your organization's business model? $n = 509$.

6. Top Third-party Breaches of 2018 (So Far) (Denver, CO: Cyber GRX, 7 June 2018), accessed at https://www.cybergrx.com/resources/blog/top-11-third-party-breaches-of-2018-so-far-data-breach-report/.

7. Q25: Have you experienced such a surprise* in the last 12 months? *An emerging or atypical risk requiring the attention of executive management that was not foreseen. $n = 435$.

8. 2018–2019 NACD Public Company Governance Survey: Key Findings (Arlington, VA: National Association of Corporate Directors, Dec. 2018), Key Finding 9, accessed at https://www.nacdonline.org/insights/publications.cfm?ItemNumber=63799.

9. Interpretation of IIA Standard 1110 — Organizational Independence (Lake Mary, FL: Institute of Internal Auditors, 1 January 2017), accessed at https://global.theiia.org/standards-guidance/attribute-standards/Pages/Attribute-Standards.aspx Also see Implementation Guide 1100: Independence and Objectivity (Lake Mary, FL: Institute of Internal Auditors, 1 January 2017), section titled "Considerations for Implementation," p. 14, accessed at https://na.theiia.org/standards-guidance/recommended-guidance/Pages/Practice-Advisories.aspx.

AUDIT EXECUTIVE
CENTER

GLOBAL HEADQUARTERS / 1035 Greenwood Blvd., Suite 401 / Lake Mary, FL 32746 / www.theiia.org/AEC

2019-1826