Internal Audit's Expanding Role

The Foundation for Connected Risk

AUDITBOARD

Table of Contents

Introduction: The Unsustainable Risk Exposure Gap

Our organizations have changed dramatically over the past five years. COVID transformed how many businesses provide their customers with goods and services. Geopolitical events continue straining supply chains, making it more difficult to provide reliable budgets, forecasts, and annual plans. Regulatory requirements in banking and financial reporting are increasing in complexity and velocity, requiring more resources to become compliant. Rapid technological advances (including generative AI) bring new opportunities for organizations to succeed while also introducing new risks and threats, including up-ending existing processes to manage intellectual property and trade secrets.

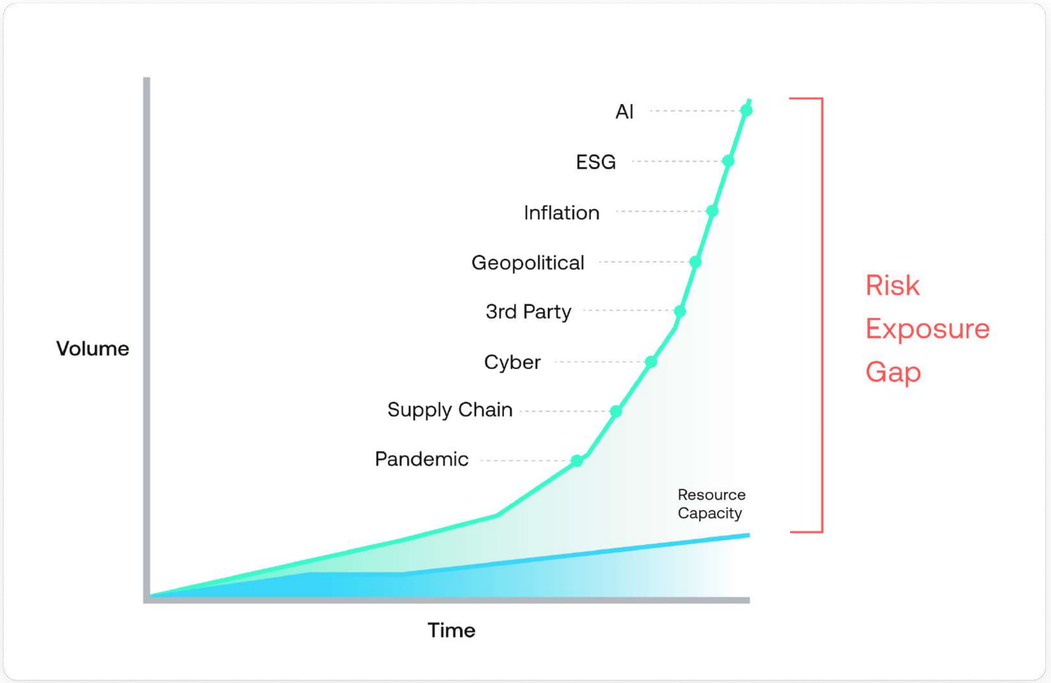
Unfortunately, this unprecedented risk landscape — characterized by pervasive uncertainty, ambiguity, and volatility — is coupled with a lack of capacity within most organizations to manage these risks to an acceptable level. **This mismatch between increasing risk demand and insufficient risk management capacity creates what we call the risk exposure gap** (see Figure 1).

The risk exposure gap can result in damaging financial and reputational impacts, including penalties from noncompliance with regulations (averaging $14M per noncompliance event), and lost revenues or market share from third-party risk incidents (averaging $1B per third-party incident); and material weaknesses that can lead to dropping share prices, valuations, and investor confidence. The most critical impact, however, is also the most common: **In most organizations, management simply isn't getting the information needed to make decisions and drive the business forward**.

Closing the risk exposure gap is no simple task. With siloed teams, manual processes, fragmented data, resource constraints, lagging technology adoption alongside rapidly increasing digital risk, and the challenges of attracting and retaining the talent needed to address emerging risks — many organizations simply lack the capabilities needed to address the gap.

To address the widening risk exposure gap, many organizations are looking to their internal audit teams for help. A 2024 AuditBoard survey of internal audit leaders[1] found that 55% of CFOs and 50% of audit committees and boards are asking internal audit to do more work around risk. But as our survey also found, the bulk of internal audit's capacity continues to be locked up in traditional audit and SOX work. Figure 2 shows that on average, **internal audit functions with Sarbanes-Oxley (SOX) responsibilities are currently allocating only 15% of their time to advisory-related work focused on key capabilities** like enterprise risk management (ERM), continuous controls monitoring, information security controls testing, corporate investigations, and others. Functions without SOX responsibilities allocate only slightly more advisory time: 21% of their total bandwidth, on average.

Figure 1. Risk Exposure Gap



[1] AuditBoard collected data from 150 respondents globally in an online survey conducted in February 2024. All respondents self-identified as a CAE or internal audit leader. Approximately 28% of our respondents were from the industrial sector, 25% from finance/insurance, 19% from services, 19% from government/education, and 10% from technology. More than 38% of our respondents were from organizations with annual revenues between $500M and $5B, 19% $50M–$500M, 12% $5B–$20B, 12% up to $50M, and 7% above $21B. Another 14% cited revenues as confidential.

At the same time, survey results clearly reflect an expanding remit: Internal auditors are already being asked by audit committees, boards, and CFOs to become involved in more advisory areas. In other words, **internal audit typically has only a small slice of its overall bandwidth to allocate to a massive (and growing) bucket of crucial advisory responsibilities**. The survey nevertheless found that internal auditors themselves believe they can and should be doing more: 61% of chief audit executives (CAEs) say they have pushed to take on more responsibilities within the past two years. **These findings could reflect a growing perspective that traditional internal audit work alone may be insufficient to help organizations close their ever-widening risk exposure gap.**

Audit teams — already stretched thin — have limited bandwidth to take on additional risk-related work or upskill teams in emerging risk areas, and open job reqs are taking longer to fill as organizations compete for a limited number of qualified candidates. If the solution isn't simply adding headcount, what's the right way forward? How can internal auditors free up time to provide more value to their organizations through the resources already allotted?

One answer is connected risk, a modern, cross-functional approach to managing risk across the enterprise. A connected risk approach enables audit, risk, and compliance teams to work smarter through integrated risk management (IRM) supported by enabling technologies that connect teams, unify data, and automate processes — and internal audit is well-positioned to take the lead. Indeed, the CAEs we surveyed self-assess IRM as the #1 area in which they should have more responsibility. But most organizations lack IRM maturity: Only 14% report having a formal IRM strategy and approach, and a mere 4% say it's working well.

Connected risk is a vital way internal auditors can create value that helps their organizations close the risk exposure gap. After all, if internal auditors don't proactively and strategically help to define the profession's evolving role, there's no guarantee they'll still be needed years down the road. This report will break down key insights on internal audit's expanding remit, evolving stakeholder expectations, and the impact on the growing risk exposure gap, and provide actionable guidance on key internal audit projects to help your organization build the foundations for connected risk.

Internal auditors have only limited bandwidth to dedicate to a fast-expanding remit.

On average, internal audit functions *with* SOX responsibilities allocate

Only 15%

of their total time to advisory work

On average, internal audit functions *without* SOX responsibilities allocate

Only 21%

of their total time to advisory work

Internal audit leaders believe they can and should do more risk-related work.

61%

of CAEs say they have pushed to take on more responsibilities

IRM

is the #1 area where CAEs self-assessed they should take on more responsibility

Key stakeholders also want internal audit to do more around risk.

50%

of audit committees or boards have asked internal audit to be more involved

55%

of CFOs have asked internal audit to be more involved

THE CHALLENGE

How can internal audit free up time to provide more value to the organization through the resources already allotted?

The Expanding Remit of Internal Audit

Current State: Capacity Limitations Collide With Expanding Responsibilities

We can't create a roadmap that gets internal auditors where we need to go before first determining where we are. To that end, AuditBoard's survey focused on understanding how internal auditors are currently spending their time between traditional responsibilities and other advisory activities, and what advisory activities are becoming more prominent. A clear picture emerged: **With an ever-expanding remit and limited bandwidth for advisory-related services, internal auditors face significant challenges in keeping pace with risk demand.**

INTERNAL AUDIT'S LIMITED TIME ALLOCATION FOR ADVISORY WORK

To understand the current state of how internal auditors are allocating their time, we categorized internal audit's work into three primary buckets: (1) SOX compliance work, (2) traditional internal audit work (e.g., risk-based internal audits, reporting, and issue follow-up), and (3) other assurance or advisory-related work. Respondents indicated what percentage of their time they spend on each. **As shown in Figure 2, the percentage of time devoted to advisory doesn't increase significantly when internal audit doesn't have SOX responsibilities.**[2]

Figure 2. Internal Audit Time Allocation — With and Without SOX Responsibilities

Headcount	TRADITIONAL AUDIT	ADVISORY	SOX
1-5	43%	15%	42%
6-10	42%	15%	43%
11-20	61%	14%	25%
21-40	43%	15%	42%
41-200	58%	16%	26%
AVERAGE	49%	15%	36%

Headcount	TRADITIONAL AUDIT	ADVISORY
1-5	81%	19%
6-10	78%	22%
11-20	84%	16%
21-40	67%	33%
41-200	85%	15%
AVERAGE	79%	21%

As Figure 2 shows, on average:

- **When internal audit does have SOX responsibilities**, 85% of their time is allocated to either SOX or traditional internal audit work, with only 15% allocated to advisory.
- **When internal audit does NOT have SOX responsibilities**, 79% of their time is allocated to traditional internal audit work, with only 21% allocated to advisory.

[2] **Question:** Of all of the resources aligned to internal audit, how are those resources allocated to the following activities?

Answer options: SOX compliance; traditional internal audit work (IA risk assessment, reporting, risk-based internal audits, issue follow-up); other assurance or advisory-related work.

IMPROVING THE PROCESS OF INTERNAL AUDIT

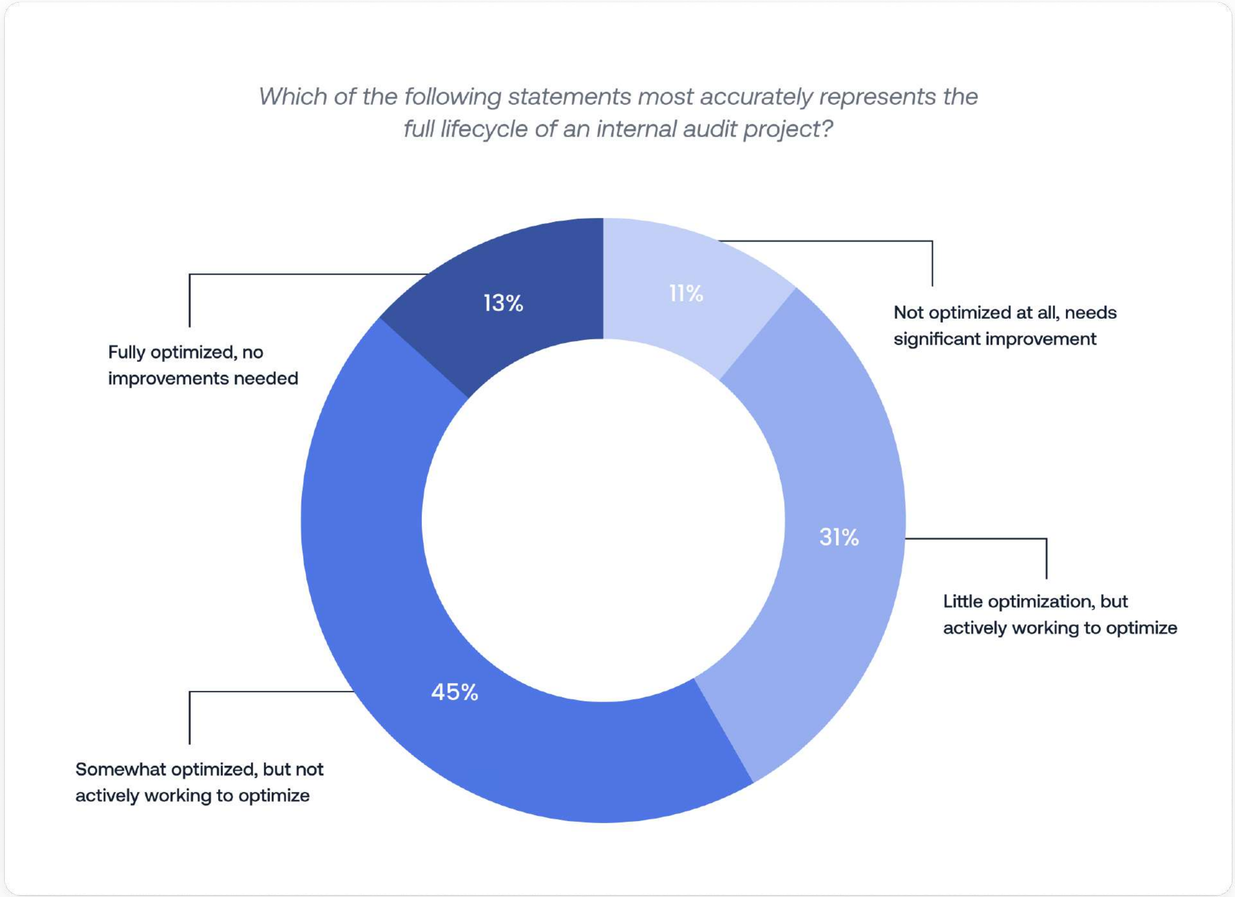
Another aspect of the AuditBoard survey aimed to understand how internal audit carries out its work, and if there are further opportunities to improve.

Surprisingly, most internal audit leaders believe they can do better: **87% of CAEs see opportunities to improve how traditional internal audit work gets done (Figure 3)**. But nearly half admit that they're not actively working toward making improvements.[3]

When asked to describe the full lifecycle of an internal audit project (i.e., planning, fieldwork, reporting, issue follow-up, ongoing interactions with audit customers):

- Only 13% of CAEs rate their processes as fully optimized.
- Another 11% admit that their processes are not optimized at all.
- Another 31% say their processes include "little optimization" but they're actively working to optimize.
- Concerningly, **nearly half (45%) of CAEs consider their processes only somewhat optimized — *but are not actively working to optimize***.

Figure 3. Internal Audit Project Optimization



[3] **Question:** Which of the following statements most accurately represents the full lifecycle of an internal audit project (i.e. planning, fieldwork, reporting, issue follow-up, and on-going interactions with audit customers)?

Answer options: Not optimized at all, needs significant improvement; little optimization, but actively working to optimize; somewhat optimized, but not actively working to optimize; fully optimized, no improvements needed.

Whether the impediments to continuous improvement stem from a lack of capacity, fear of change, or lack of resources, the stance that "this is the way we've always done it" is growing obsolete. Remaining relevant and creating value for organizations means continuing to innovate how internal audit's work gets done. **Like it or not, simply maintaining the status quo is insufficient for helping our organizations close the risk exposure gap.**

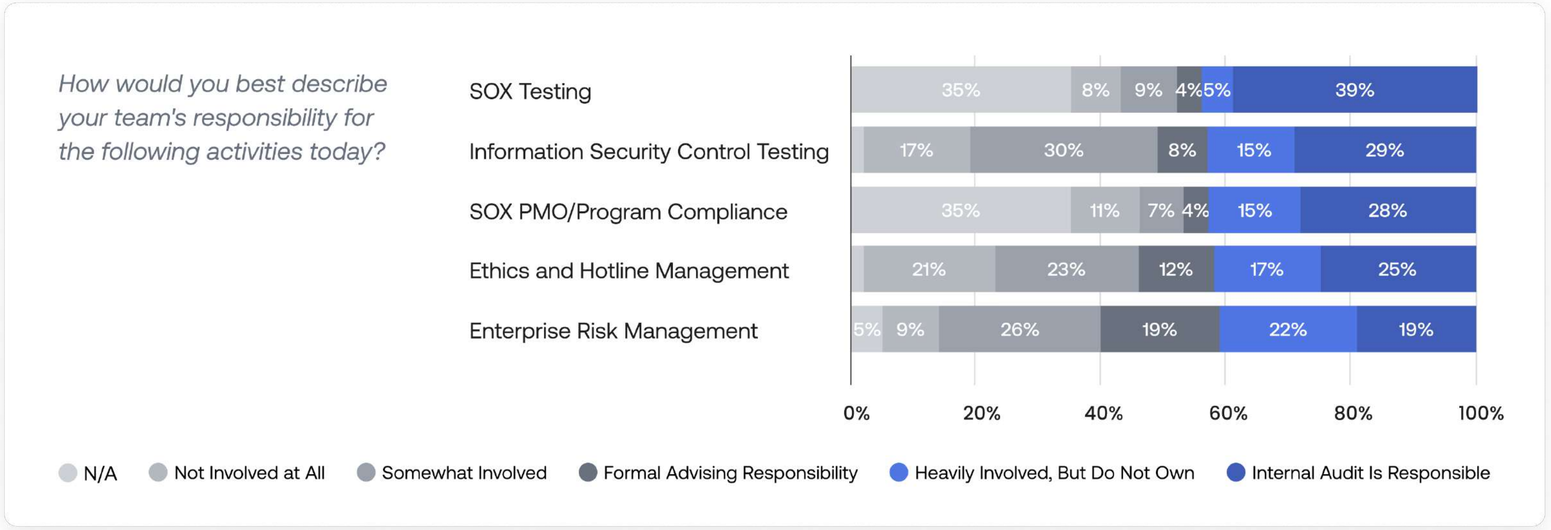
INTERNAL AUDIT'S RESPONSIBILITIES HAVE EXPANDED IN KEY AREAS

Internal audit's remit is expanding as organizations struggle to adapt and respond to today's highly volatile risk landscape. CAEs described their current responsibilities beyond traditional internal audit work across 24 wide-ranging categories. Figure 4 reflects the top five most common responsibilities and internal audit's corresponding degree of involvement.

This breakdown of responsibilities suggests that:

- **Unsurprisingly, SOX remains a dominant responsibility.** Across all organizations, SOX testing ranked #1, and SOX PMO/program compliance ranked #3. In addition, 66% of public company CAEs surveyed either own or are heavily involved in SOX testing, and 49% either own or are heavily involved in SOX PMO/program compliance.
- **Information security control testing appears to be growing in importance.** Somewhat surprisingly, information security control testing came in at #2, with 82% of CAEs involved in some capacity and 44% either owning or heavily involved. This high rank could be due to IT General Controls (ITGC) testing or reflect an increase in internal audit assistance around other information security controls (e.g., PCI compliance, AICPA trust standards, ISO/NIST controls testing). It could also reflect smaller teams with more crossover responsibilities — as in, people wearing many different hats simultaneously.
- **ERM focus still isn't where it needs to be.** ERM ranked #5, with 41% of CAEs owning or heavily involved and another 19% formally advising. Now, consider that ERM is aligned with advisory in these responses — meaning that the 60% of CAEs who are owning, heavily involved, or formally advising must perform this work within the 15–21% time internal auditors typically allot to advisory. This is insufficient to help close the risk exposure gap.
- **Continuous monitoring deserves greater internal audit focus.** Only 28% of CAEs either own or are heavily involved with continuous monitoring of a key process, but 60% of surveyed auditors have some level of involvement in ERM — and 40% have no involvement whatsoever. This presents a key opportunity for improving internal auditors' competencies in facilitating ERM programs. Given the criticality of continuous monitoring for effective risk management in today's risk landscape, this finding should be eye-opening.

Figure 4. Top Five Responsibilities Beyond Traditional Internal Audit Work



In other words, **in many organizations, ERM is most likely not getting the attention it requires.** Of the organizations surveyed, 95% have ERM programs, and they're often delegated to internal audit: 60% of surveyed CAEs have some level of involvement in ERM for their organizations. Are these internal audit leaders able to give ERM the time it deserves when on average they have such limited bandwidth to devote to all advisory work? **To ensure internal audit's work remains focused on the right risks at the right times, internal audit must free up more time to focus on risk initiatives.**

---

[4] **Question:** From the table below, how would you best describe your team's responsibility for the following activities?

Answer options: Internal auditing; SOX testing; SOX PMO / program compliance; ERM; ORM; IRM; information security control testing; cyber security program compliance; IT risk management; third-party risk management; data privacy compliance; ESG compliance; compliance control / transaction testing; compliance risk assessments; ethics and hotline management; corporate investigations; supply chain risk management; distributor / supplier / customer audits; quality assurance; data loss prevention; governance over new programs/initiatives; physical security; continuous monitoring of a key process; IT program governance; data management / analysis.

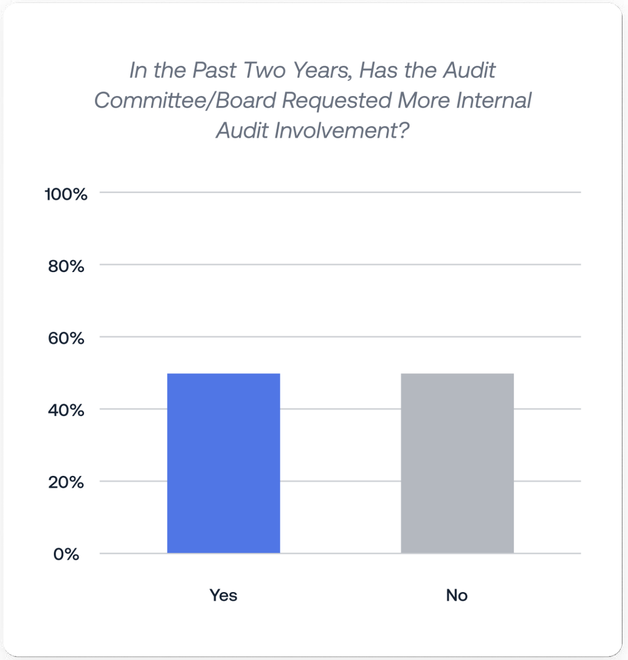
EVOLVING EXPECTATIONS FROM ALL DIRECTIONS

Internal audit also faces changing expectations from many of its key stakeholders:

Half of CAEs indicate that their audit committee or board has asked internal audit to be involved in more activities in the past two years (see Figure 5).[5]

Key areas included environmental, social, and governance (ESG), ERM, governance (including AI governance), cybersecurity, investigations, data analytics, regulatory changes, and continuous monitoring. Notably, these are all risk-related areas.

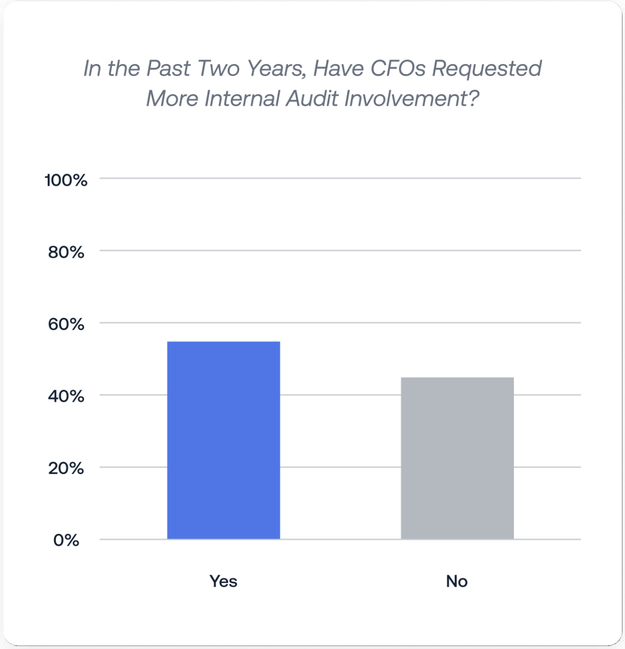
Figure 5.



More than half (55%) of CAEs indicate that their administrative reporting managers (typically CFOs) have asked internal audit to be involved in more activities in the past two years (see Figure 6).[6]

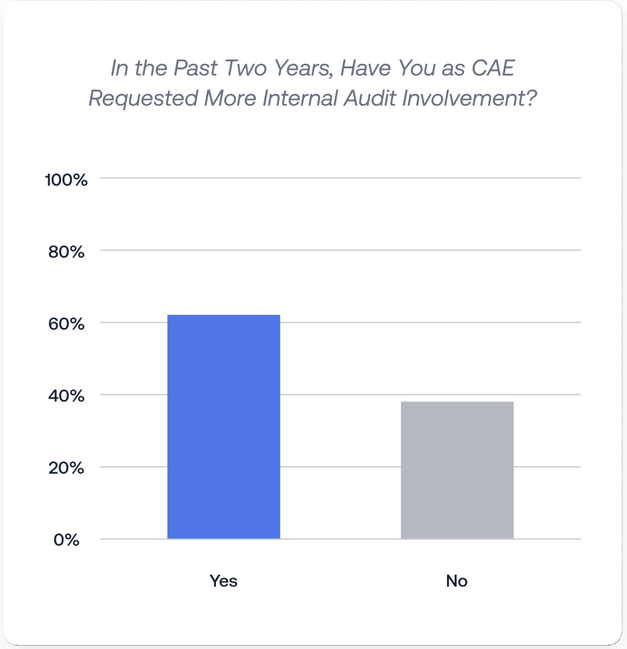
Key areas included ERM, ESG, governance, operational initiatives, and quality assurance.

Figure 6.



CAEs themselves believe they should be doing more (see Figure 7), with 61% saying they have pushed to take on more responsibilities over the past two years.[7]

Figure 7.



[5] **Question:** Has the audit committee/board of directors asked for internal audit to be involved in more activities in the past two years?

[6] Has internal audit's administrative reporting manager asked for internal audit to be involved in more activities in the past two years?

[7] Has internal audit pushed to take on more responsibilities in the past two years?

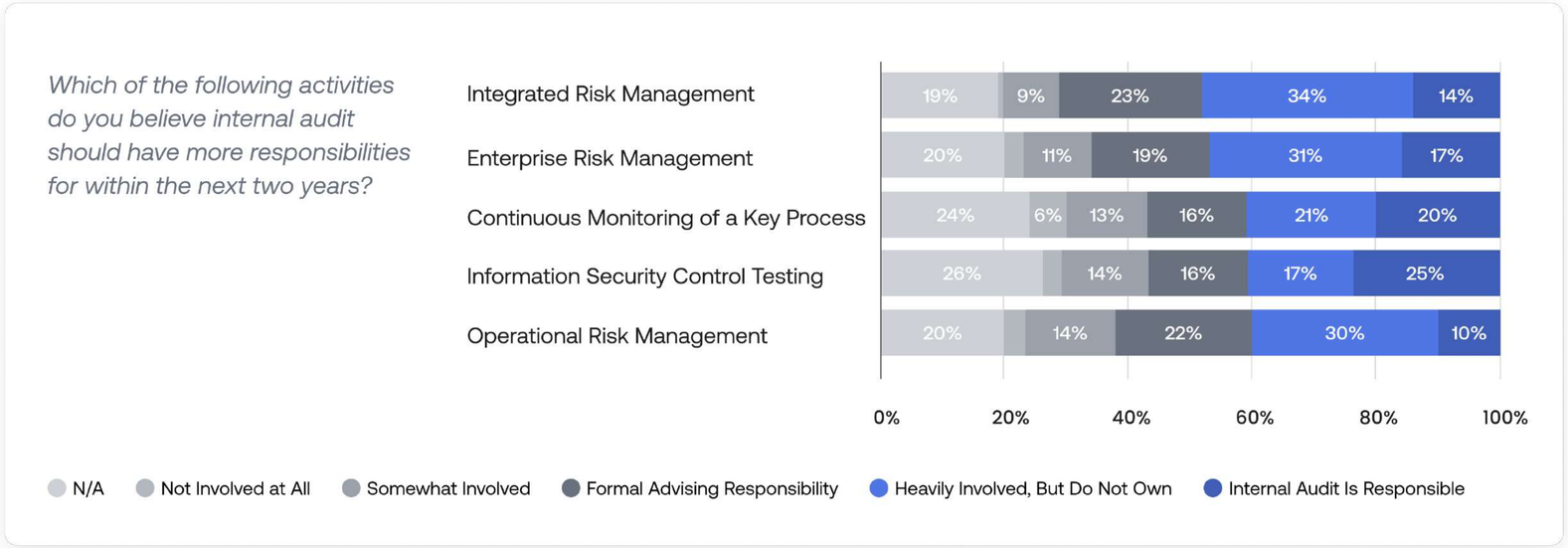
We asked internal audit leaders to identify the areas in which they believe internal audit should have more responsibilities within the next two years.[8] See Figure 8 for key takeaways.

As shown in Figure 8, **IRM was CAEs' #1 choice** for where they should be more involved. Notably, however, IRM is not even reflected in auditors' top existing responsibilities (see Figure 4), though it was an answer option. CAEs' #2 choice — ERM — is also telling. **There seems to be a growing consensus that internal audit needs to level up its ERM game** (e.g., limited involvement graduating to heavy involvement or even owning). In aggregate, these findings suggest:

- **A need for greater overall risk focus from internal audit**, since three of the top five areas relate to becoming more involved with risk work — IRM, ERM, and ORM.
- **A need for increased use of data analytics** reflected in the #3 rank of continuous monitoring of a key process.

In sum, audit committees, boards, and CFOs are all asking internal audit for more risk-related work just as CAEs themselves are pushing to take on more risk-related work. **This is a clear business case for internal audit to not only take on this work, but to take a leading role in driving connected risk approaches to help close the risk exposure gap.** Part 2 of the report takes a closer look at the forces contributing to the risk exposure gap, how connected risk helps to close it, and how internal audit can play a vital role in spearheading a connected risk solution.

Figure 8. Top Five Areas Where CAEs Seek Greater Responsibilities



[8] **Question:** From the table below, which of the following activities do you believe internal audit should have more responsibilities in within the next two years?

Answer options: Internal auditing; SOX testing; SOX PMO / program compliance; ERM; ORM; IRM; information security control testing; cyber security program compliance; IT risk management; third-party risk management; data privacy compliance; ESG compliance; compliance control / transaction testing; compliance risk assessments; ethics and hotline management; corporate investigations; supply chain risk management; distributor / supplier / customer audits; quality assurance; data loss prevention; governance over new programs/initiatives; physical security; continuous monitoring of a key process; IT program governance; data management / analysis.

IRM Maturity Is Lacking at Most Organizations

While surveyed CAEs select IRM as their top choice for increasing responsibilities, **most organizations still have a long way to go toward IRM maturity**. As Figure 9 shows, our survey found that many audit, risk, and compliance functions are still largely working in silos or collaborating informally and inconsistently, with no formal strategy connecting efforts or enabling improved collaboration.[9]

Of note, surveyed CAEs indicate that:

- **Fully 96% of organizations lack mature IRM programs.** Only 4% of CAEs reported having an IRM strategy and approach that is working well.
- **Eleven percent of organizations report having no IRM strategy whatsoever**, with audit, risk, and compliance functions working independently.
- **A little over half are seemingly stuck in the status quo:** 51% of organizations seem to know IRM is needed, but have no cohesive strategy for it. This figure includes 29% reporting that functions are informally sharing data and perspectives, and 22% saying that some but not all functions are working together.
- **Another 24% have no formal strategy, but say they're actively working toward connecting audit, risk, and compliance functions.** This finding is promising, reflecting a recognition of the need for IRM even if they aren't yet using the specific term.
- **Only 14% report having a formal IRM strategy and approach — but of this amount, 10% say it needs improvement.** This lack of IRM maturity indicates a massive opportunity for internal audit to provide value.

Figure 9. Organization's Current State of IRM

Which of the following most closely aligns with your organization's current state of Integrated Risk Management?

These findings reflect a significant shift toward improved collaboration between the audit, risk, and compliance functions. **The imperative to work together is becoming increasingly apparent, leading many organizations to place greater emphasis on sharing data and perspectives between — as well as formally connecting — functions.** Still, these findings are a clear call to action: Are you doing the right work in the right ways? Or can you change how you've ordinarily gotten things done to create more capacity to provide value to your organization? In the next section, we offer guidance on using connected risk to enable increased risk management capacity, breaking down practical steps internal auditors can take to build the right foundations.

[9] **Question:** Which of the following most closely aligns with your organization's current state of Integrated Risk Management / Combined Assurance / Connected Risk?

Answer options: We don't have a strategy - all departments with audit, risk, or compliance responsibilities work independently; leaders from audit, risk, and compliance functions informally share data and perspectives, but a formal IRM / connected risk strategy or process does not exist; there are some functions that work more closely together and well, but not all functions; we are actively working to combine / consolidate / integrate / connect all major audit, risk, and compliance functions at our company; we have an integrated risk management strategy and approach, although improvement is needed; we have an integrated risk management strategy and approach, and it is working well.

Future State: Internal Audit Takes the Lead on Connected Risk

WHY CLOSING THE RISK EXPOSURE GAP IS SO DIFFICULT

Siloed teams, disconnected data, labor-intensive manual processes, budget and resource constraints, lagging technology adoption alongside rapidly increasing digital risk — these and other factors make closing the risk exposure gap incredibly challenging.

Again, risk management capacity simply isn't keeping pace with demand in most organizations. Audit, risk, and compliance teams — already stretched thin — have limited bandwidth to take on additional risk-related work or upskill teams in emerging risk areas. Further, these teams are often relying on legacy processes and technologies that limit agility, productivity, collaboration, and access to real-time information and insights. This often results in outsized efforts expended in the wrong areas, duplication of efforts, audit fatigue, and different perspectives from different audit, risk, and compliance teams. **How can business leaders make effective decisions when they're getting conflicting information from their various trusted advisors?**

HOW CONNECTED RISK HELPS CLOSE THE RISK EXPOSURE GAP

The solution is a new and emerging strategy for organizations to better manage risk: **connected risk, a modern, cross-functional approach to managing risk across the enterprise**. Connected risk solves for the risk exposure gap by breaking down silos, increasing alignment, enabling collaboration and information sharing, unifying data, and automating key processes.

Purpose-built, intelligent technology solutions like AuditBoard help increase adoption from risk and control owners while increasing reliance, reducing audit fatigue, providing improved visibility on risks, controls, and potential weaknesses, streamlining compliance work, and enabling continuous risk monitoring — all crucial capabilities for helping organizations scale the risk exposure gap. **Connected risk also empowers stakeholders with the real-time data, insights, and context they need to make better business decisions and provide effective oversight.**

Connected Risk Fundamentals

What's the difference between IRM and connected risk? While IRM and connected risk share several goals, including shared data, collaboration between teams, and an integrated, organization-wide view of (and approach to) risk management, **connected risk relies on modern and intelligent technology predicated on a single platform that spans all teams to manage risk across the enterprise**. Connected risk also uses intuitive, purpose-built capabilities (e.g., automation, AI, solutions based on practitioner expertise) to unlock new value creation opportunities.

In many organizations, however, IRM efforts are still aligned with legacy approaches relying on disconnected, bolt-on technologies that actually create obstacles to collaboration. **Since these legacy tools don't work together or share data, they tend to harden rather than break down silos.** They also lack the purpose-built automation — a core capability of connected risk — that helps teams share workflows and operate with greater impact. Further, without a unified data core operating across teams, bolt-on IRM solutions make it impossible to effectively leverage AI at an organizational level to surface timely alerts, actionable insights, and informed recommendations.

Learn more about how AuditBoard's connected risk platform can elevate how your audit, risk, InfoSec, and ESG teams work together to manage risk more effectively, and request a tailored product walkthrough to see it in action.

WHY INTERNAL AUDIT SHOULD TAKE THE LEAD

The CAEs we surveyed believe they have a responsibility to help connect their audit, risk, and compliance colleagues' views of risk. They recognize it as an opportunity to help their organizations manage risk more effectively. Indeed, business-critical risk should be a top priority for every internal auditor.

Taking the lead on connected risk is a natural evolution of internal audit's role.

Because of our subject matter expertise testing financial reporting controls, internal audit took the lead with SOX compliance following the Sarbanes-Oxley Act of 2002. Over time, our expertise naturally expanded into governance, risk, and compliance (GRC), deepening our cross-functional business acumen and relationships. As a result, internal audit is positioned to add tremendous value in areas requiring cross-functional collaboration and knowledge.

Further, the new Global Internal Audit Standards may suggest that internal auditors need to better understand their organizations' governance, risk, and control framework (Standard 9.1), that their internal audit plan needs to be risk-focused (Standard 9.4), and that internal audit should have a strategy to coordinate and rely on the work of other assurance providers (Standard 9.5).

Taking the lead on connected risk also elevates internal audit's importance to the business.

Audit committee chairs want internal auditors to be trusted advisors who regularly share their perspectives, connecting the dots to help them understand the bigger picture of how the organization is managing risk. They also want internal auditors to be aligned with other risk and control functions (or be ready to explain why they aren't), and courageous in bringing important matters to their attention.

Internal audit has a unique perspective that enables us to see across the organization, and to serve as the trusted advisors business leaders may not know they have. But risk management capacity limitations aren't going away, and adding headcount doesn't necessarily solve the problem. So, internal audit's new mission is to **architect connected risk environments that enable more effective, efficient risk management, thereby freeing up time from SOX and traditional audit work and enabling internal audit to invest more time in the value-add advisory activities organizations urgently need.** Here's how.

The Connected Risk Journey: Best Practices for Getting Started

The general roadmap below can help you build the business case and foundations for connected risk. The idea is to start small, gaining credibility and traction as you lay the necessary groundwork. First, get internal audit's house in order. Next, undertake four key projects that are proven leading practices for building the foundations for connected risk. Then, get started with connected risk quick wins to gain buy-in, demonstrate value, and begin implementing connected risk across the organization.

Set the Stage for Connected Risk: Modernize Internal Audit

Internal audit's reputation for controls management will be a factor in adoption of connected risk in other parts of the organization. Accordingly, before turning your focus to helping others improve their processes, begin by cleaning up your own backyard in two key areas.

1. REDUCE TIME SPENT ON SOX

If your internal audit function is responsible for SOX, are you doing everything you can to reduce the time you're spending on it? As parts one and two of this article series explain, you can uplevel your function's SOX approach by focusing on six core tenets:

- **Educate** control owners to help prevent control deficiencies (e.g., training, observation, involvement in risk assessments).
- **Automate** routine tasks (e.g., status updates, reporting, evidence collection, control certifications) with GRC technology.
- **Delegate** appropriate responsibilities (e.g., data collection, control testing, project management) to colleagues in Finance, Operations, or IT, or consider peer testing strategies.
- **Eliminate** work that isn't needed (e.g., certain processes or controls for in-scope entities, certain audit reports) according to your annual SOX risk assessment.
- **Advocate** for your SOX program by sharing positive control performance (e.g., newsletter) and gamifying SOX work.
- **Increase reliance** by working with the external auditor to increase their reliance on management's work.

2. OPTIMIZE INTERNAL AUDIT ACTIVITIES

Again, only 13% of the CAEs we surveyed felt their functions were optimized. Ask yourself:

- Does internal audit have an actionable strategic plan that is actively supported by working to achieve key performance metrics?
- Are internal audit's efforts focused on the risks that matter?
- Is significant time spent manually reviewing and approving test steps?
- Does your department lack capabilities to provide real-time reporting on testing status, audit completeness, and issue resolution?
- Are there automated notifications and reminders to notify audit customers of items required from them, including document requests, audit surveys, and needed action plans?
- Are audits completed by trained auditors who have the appropriate competencies and expertise? If not, are training plans developed and linked to the audit plan to ensure audits are completed by those with the needed skill sets?

Connected Risk Current-State Assessment: Four Foundational Projects

Once internal audit's house is in order, you're ready to complete four fundamental projects that help to establish a strong foundation for your organization's connected risk program.

1. DATA GOVERNANCE REVIEW

Business data is foundational to connected risk, but organizations today create more data than ever. To suitably manage some of your organization's key risks, it is vital to understand what your organization's key data is. **A data governance review enables you to establish a baseline understanding of an organization's key data, how it is being collected, shared, stored, and protected across your organization.**

KEY QUESTIONS TO ANSWER

Document your organization's key risk data, creating an inventory that captures all of the following:

- What is your organization's key data? Key data typically includes intellectual property, IP, and other data that if lost, stolen, or destroyed, would have a signficant negative impact to your business.
- Where is the data located (i.e., network or physical location)?
- Who has access to the data?
- What controls are in place to protect and monitor the data?

2. ASSURANCE MAPPING

In order to connect risk data, workflows, and reporting, you'll need to **understand who is performing assurance work for your organization's key risk and controls**. Having a documented assurance map is the easiest and most effective tool to accomplish this. Outlining which internal and external teams provide assurance over your organization's key risks will help identify areas of duplicative effort, and perhaps more important, a lack of needed assurance in key risk areas.

For those assurance teams that have a robust assurance process and document their work in a similar nature to internal audit, there may be opportunities for internal audit to decrease their workload and rely on the other assurance provider's work. Global Internal Audit Standard 9.4 (Coordination and Reliance) recommends assurance mapping.

KEY QUESTIONS TO ANSWER

Create a map of your organization's risk assurance program, documenting all of the following to identify coverage gaps, duplicative work, and opportunities:

- What are your organization's key risk areas?
- What assurance and advisory teams provide assurance over these risk areas? This is to include both internal and external assurance providers.
- What controls, workflows, processes, strategies, and projects do these teams have for each risk area?

3. TECHNOLOGY AND MATURITY ASSESSMENT

Technology is critical for any connected risk program. If it's not easy to share data across different applications, consideration should be given to leveraging a purpose-built audit, risk, and compliance platform. Such platforms also open up opportunities for leveraging automation, data analytics, and generative AI, as well as for automating and consolidating reporting, providing real-time information and insight to help inform better business decisions.

KEY QUESTIONS TO ANSWER

Inventory the technologies currently being used to help you understand your organization's ability to connect internal and external data sources and share data across applications. Document and assess:

- What audit, risk, and compliance applications are being used in the organization?
- Can data easily be shared across applications? For example, can data in an application used to manage IT security controls feed into another application being used to manage enterprise risk?
- What level of effort and costs are required to periodically update each application's data? For example, do updates require resource-intensive manual uploads or expensive APIs or software resources to ensure real-time feeds from one application to another?

4. SHARED RISK DEFINITIONS

Risk and assurance groups that have been operating in silos often use different definitions and scorecards to categorize, qualify, and quantify the same risks. **Foundational elements of connected risk include having one definition of risk shared by the enterprise, as well as a common approach to quantify and assess risk.**

KEY QUESTIONS TO ANSWER

If your organization is like most, the first three projects are likely to surface a range of risk definitions and scoring systems. Assess the different systems to agree on a shared risk taxonomy that addresses all of the following:

- What different ratings (e.g., high, medium, low; stoplights; color coding) are being used to score risks, and how is each defined? What ratings and definitions can be used to create a consistent taxonomy and common language going forward?
- What risk attributes are different teams considering in their risk assessments? What common attributes can be agreed on for use in future risk assessments?
- Are there established thresholds for risk appetites and a risk tolerance?
- What KRIs do teams use? What shared KRIs can teams use going forward?

Quick Wins: Organize, Connect, Coordinate, and Evangelize

Once these four foundational projects are complete, what's next? **Focus on quick wins that can help you gain buy-in and showcase connected risk's value and potential across the organization.** Based on interviews with over 40 risk, control, and assurance leaders on the topic of connected risk, Figure 10 illustrates key data and team efforts that must be aligned to advance a connected risk approach.

Figure 10. Connected Risk: Where to Start

ORGANIZE WITHIN INTERNAL AUDIT

The absolute best way to get connected risk quick wins is to **begin with areas under your own remit**. For example:

- Can SOX controls and risk statements be unified with other operational, compliance, and strategic risks and controls being tested in risk-based audits?
- Create a shared list of issues across SOX and internal audit (and risk action plans, if ERM is under internal audit's remit).
- Do audit and advisory projects on the audit plan clearly align to the audit universe, key enterprise risks, and corporate goals, strategies, and objectives?

COORDINATE WITH OTHER SECOND-LINE AUDIT, RISK, AND CONTROL FUNCTIONS

With these foundations in place, you're ready to approach other second-line functions to explore how you can improve coordination across teams. Be strategic in your outreach based on what makes sense for your organizational structure and relationships.

For example, some internal audit functions may decide to approach risk management or compliance first. Another good option, however, is to approach information security. **In the current risk environment, CISOs and internal auditors have important opportunities to partner to advance the control environment.**

As technology, AI, cybersecurity risk and compliance, and related governance continue to evolve at lightning speed, information security teams are often strained to address their remit.

Opportunities for internal audit to help lighten their load may include information security controls documentation, control testing-related work, managing issue remediation processes, facilitating IT risk assessments, and — perhaps most importantly — integrating information security into the organization's overall connected risk approach. **Plus, if you get information security onboard, it's likely to be easier to get meetings with other second-line teams in the organization.**

EVANGELIZE ACROSS THE ORGANIZATION

Continuously evangelize the value of connected risk, coaching upwards and outwards as needed. Identify and cultivate champions across the organization, slowly building your connected risk tribe. Champions may be found:

- **First line** — Look for people with control, risk, audit responsibilities.
- **Second line** — Seek out like-minded audit, risk, and compliance leaders that are likely to understand the need.
- **Executive management, board, and audit committee** — Use external benchmarking information about competitors or other leading companies to show what other organizations are doing.

Internal Audit's Expanding Remit Should Include Taking the Lead on Connected Risk

Audit committees, boards, CFOs, and other key stakeholders all want internal audit to do more around risk. Beyond seeking assurance on risks and controls in more areas of the organization, they want internal audit's help in "connecting the dots" to gain a clearer picture of how the organization is managing its risk. Getting risk management right is essential for driving better business decisions. Internal audit doesn't need to have all the answers — but we do need to be able to surface the insights and information our organizations' leaders need to make decisions. We need to keep our leaders from having to ask, "Why didn't I know about this?"

Organizations must be more proactive, strategic, and forward-looking in how they approach risk management to remain resilient. Addressing the risks we know about — as well as those continually emerging — requires rethinking how we maximize the impact of our risk resources. This mandates increasing alignment, communication, and collaboration between audit, risk, and compliance teams, creating a necessary blurring between the second and third lines. A connected risk approach linking teams, data, and processes is the logical choice for organizations seeking to close the risk exposure gap.

Internal audit is also a logical choice to lead organizations in adopting connected risk. It fits our skill sets, engages our strengths, and aligns well with internal audit's expanding remit, and our stakeholders' desire for internal audit to focus on more risk-related activities.

- **Internal auditors are organizations' governance, risk, and compliance experts.** Connected risk — which unifies all three — is a natural extension of our expertise.
- **Internal auditors bring the cross-functional knowledge and relationships** needed to gain buy-in, connect teams and efforts, and showcase the value of connected risk.
- **Business leaders need more timely insights to be able to connect the dots more quickly and easily.** A connected risk approach provides the second and third lines with enhanced capabilities to identify, track, and report on insights, threats, and opportunities. Plus, this is a top expectation audit committee chairs have of internal audit.
- **Organizations need to increase risk management capacity to close the risk exposure gap.** The talent crisis, resource constraints, and accelerating risk velocity and volatility mean that most organizations must find ways to drive more value from the resources they already have. Connected risk enables organizations to optimize time spent on audit and control activities, improve cross-functional risk visibility, coverage, and monitoring, reduce duplication of effort and audit fatigue, and make better decisions.

***Not* investing in connected risk is a risk in and of itself.** Ten years from now, the leaders of our profession will be those who today are leading — if not architecting — their organizations' connected risk efforts. Connected risk is a journey; no organization can do everything all at once. The important thing is getting started. **Be the connected risk visionary and architect your organization needs to get on the path to closing the risk exposure gap.**

About the Author

Tom O'Reilly
Field Chief Audit Executive and Connected Risk Advisor
AuditBoard

Tom O'Reilly is the Field Chief Audit Executive and Connected Risk Advisor at AuditBoard. In his role, Tom meets with the AuditBoard Community and customers, collaborates on internal audit and connected risk strategies, and shares tactics to enhance internal audit practices and improve the coordination between second and third line functions.

Prior to AuditBoard, Tom was the Director of Internal Audit and Chief Audit Executive at Analog Devices, a Fortune 500 company, where he was responsible for leading a risk-based audit team and ERM. Tom was also an Internal Audit Manager in EY's Risk Advisory practice. While working as a CAE at Analog Devices, Tom founded the CAE Leadership Forum, a New England-based group of 200+ CAEs and internal audit leaders who met bi-monthly to share perspectives and best practices and learn from internal audit subject matter experts.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, compliance, and ESG management. Nearly 50% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fifth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.