Natural Allies

Nurturing Cyber Resilient Cultures Through Internal Audit and Information Security Collaboration

AUDITBOARD

Internal Audit FOUNDATION

Executive Summary

Cybersecurity remains a top challenge for any organization that leverages technology — a reality that encompasses nearly all modern businesses, from startups to enterprises. As a result, exploiting cyber vulnerable organizations has become big business.

In 2023, more than 3,200 data compromises were reported in the U.S. alone, affecting more than 350 million individuals.[1] Three primary avenues for cyberattacks remained phishing, credential exploitation,[2] and vulnerability exploitation, and the costs for such attacks are alarming. Median losses associated with ransomware and extortion incidents were $46,000.[3] Despite the clear-and-present danger, companies were slow to respond to known threats. In 2023, the average time to remediate 50% of critical vulnerabilities after patches were made available was 55 days![4]

Not surprisingly, cybersecurity remains the top-ranked risk among internal audit leaders globally, according to the Risk in Focus 2025 report.[5] Nearly three in four (73%) identified cybersecurity as one of the top five risks for their organizations, far outpacing the second most cited risk, human capital (51%). Similarly, AuditBoard's annual Focus on the Future report found 82% of respondents rated cybersecurity risks as "very high" or "higher than average" going into 2025.[6]

Internal audit leaders are not alone in ranking cybersecurity as a top risk. Ransomware attacks were a leading cybersecurity risk among chief information security officers (CISOs), according to a 2024 global survey, with roughly 41% naming it as one of the three major cybersecurity threats. Another 38% found malware to be a significant risk to their organizations' cybersecurity.[7]

Increasingly, risk managers recognize that holistic approaches to cybersecurity are foundational to building cyber resilient organizations. Effective cyber risk management demands alignment, transparency, and collaboration across the organization, particularly between internal audit and information security. Collaboration between these two natural allies offers diverse benefits, and recent survey data reflect that these cyber stakeholders are joining forces at many organizations. More than 80% of respondents to the 2025 North American Pulse of Internal Audit survey reported that meetings between internal audit and information security are common. The survey outcomes also reveal a strong association between the frequency of meetings and the effectiveness of the relationship between internal audit and information security.

What's more, internal audit and information security leaders from two virtual roundtable

1 "Annual number of data compromises and individuals impacted in the United States from 2005 to 2023," A. Petrosyan, Statista.com, November 2024.

2 Verizon's 2024 Data Breach Investigations Report.

3 ibid

4 ibid

5 "Risk in Focus 2025," Internal Audit Foundation, 2024.

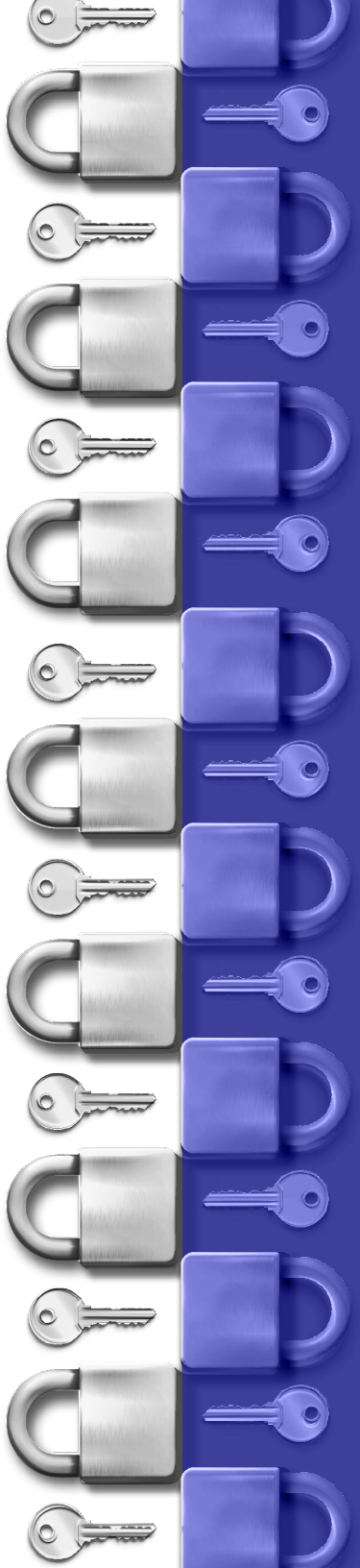
6 "Focus on the Future," AuditBoard, 2024.

7 "Most significant cybersecurity threats in organizations worldwide according to Chief Information Security Officers (CISO) as of February 2024," Statista.com, https://www.statista.com/statistics/1350460/cybersecurity-threats-at-companies-worldwide-cisos/

discussions hosted by the Internal Audit Foundation (Foundation) and AuditBoard in November 2024 emphasized the significant benefits of developing strong, collaborative relationships. These frontline leaders on the cyber battlefield eagerly shared various benefits from their partnerships, including aligned risk assessments, improved regulatory compliance efforts, combined assurance, and better communication with the board. Collaboration also plays a key role in addressing shared challenges in building cyber resilient cultures. Direct quotes from roundtable participants are found throughout this report.

Natural Allies: Nurturing Cyber Resilient Cultures Through Internal Audit and Information Security Collaboration examines the advantages of internal audit and information security relationships, offering actionable strategies for building effective collaboration. Additionally, it explores how collaboration can enable cyber resiliency and sets out goals for achieving an ideal state in the internal audit-information security relationship. Enriched by insights from 11 industry leaders who participated in roundtable discussions, the report also incorporates initial findings from the Foundation's 2025 North American Pulse survey. This survey reflects the perspectives of 406 internal audit leaders across the region and was conducted between October and November 2024.

Consider sharing this report with colleagues in internal audit or information security to spark meaningful conversations about strengthening collaboration and enhancing your organization's cyber resilience.



Collaboration between these two natural allies offers various benefits, and recent survey data reflect that these cyber warriors are joining forces at many organizations.

AUDITBOARD Internal Audit FOUNDATION

SURVEY RESULTS AND ROUNDTABLE FEEDBACK:

Insights and Connections

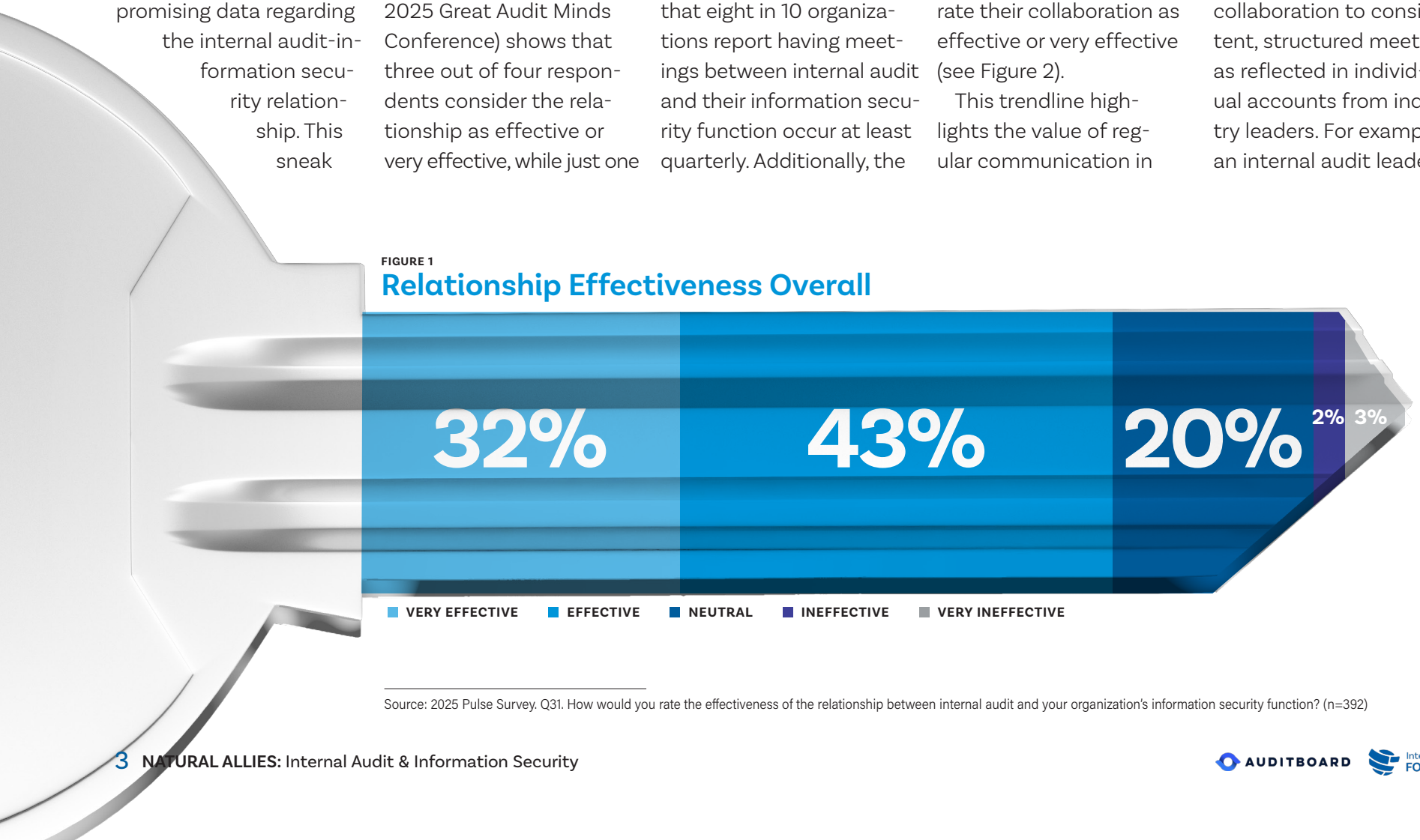
Findings from the 2025 North American Pulse of Internal Audit survey reveal promising data regarding the internal audit-information security relationship. This sneak peek into the survey's results (with full results to be released at The IIA's 2025 Great Audit Minds Conference) shows that three out of four respondents consider the relationship as effective or very effective, while just one in 20 rate it as ineffective or very ineffective (see Figure 1).

The survey results show that eight in 10 organizations report having meetings between internal audit and their information security function occur at least quarterly. Additionally, the data indicate that organizations with more frequent meetings are more likely to rate their collaboration as effective or very effective (see Figure 2).

This trendline highlights the value of regular communication in fostering strong partnerships. Many organizations attribute their successful collaboration to consistent, structured meetings, as reflected in individual accounts from industry leaders. For example, an internal audit leader

FIGURE 1

Relationship Effectiveness Overall



Source: 2025 Pulse Survey. Q31. How would you rate the effectiveness of the relationship between internal audit and your organization's information security function? (n=392)

from a food manufacturing company said she finds great value in her weekly meetings with her chief information security officer (CISO) because they keep her on the leading edge of the organization's cybersecurity efforts.

"I find they're a very good partner because they're on the front end of project implementations, whether it's putting a firewall in one of our plants or replacing an enterprise software," she said. "From a strategic perspective, we share a lot of information that way."

This insight highlights how close partnerships enable information sharing and can provide internal audit with early visibility into critical projects.

Meeting Frequency

Greater meeting frequency enables stronger collaboration. Many participants of the Foundation and AuditBoard roundtable report having bi-weekly or monthly scheduled meetings but also described ad hoc meetings or joint sessions with the chief financial officer or other C-suite executives. For some, the increased meeting frequency and the effectiveness of the internal audit-information security relationship are built around committees that include leaders from many relevant parts of the organization.

An audit, risk, and compliance leader shared that his healthcare organization fosters collaboration through various committees dedicated to leaders in information security, information technology (IT), compliance, risk, and internal audit. These committees provide regular opportunities for leaders to engage on information security and risk, and compliance and privacy.

"We're making sure that there is tight connection between those groups where they're frequently talking, not just formally about agenda topics, but about the day-to-day and what's going on," he said.

Indeed, research in fields as varied as patient care, disaster response, and software engineering find ad hoc communication is a key component to stronger collaboration.

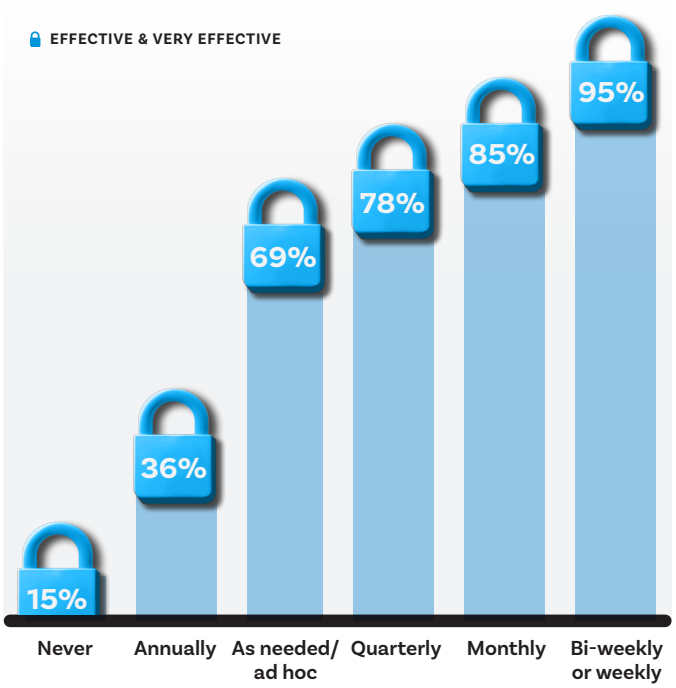
Deviations

Public sector auditors, younger audit leaders buck trends. The results from the 2025 Pulse survey also reveal two relevant deviations in the internal audit-information security relationship. The first finds the lion's share of public sector respondents rate their relationships with information security as neutral (see Figure 3), with fewer than six in 10 (53%) rating it as effective or very effective.

This data point unveils a significant opportunity for public sector audit leaders. Indeed,

FIGURE 2

Relationship Effectiveness & Meeting Frequency



Source: 2025 Pulse Survey. Q30. How frequently does internal audit meet with your organization's information security function to discuss security issues? by Q31. Very effective and effective. (n=375)

> "Sometimes pain brings people together."
>
> –Internal audit leader on how cyber incidents influenced the internal audit-information security relationship at her organization.

public sector auditors and CISOs at the roundtables emphasized significant potential and benefits of their relationships.

The CISO of a public transit authority expressed high praise for the strong relationship with internal audit that he inherited upon taking the role. The chief risk and audit officer had already established an enterprise risk management office and program.

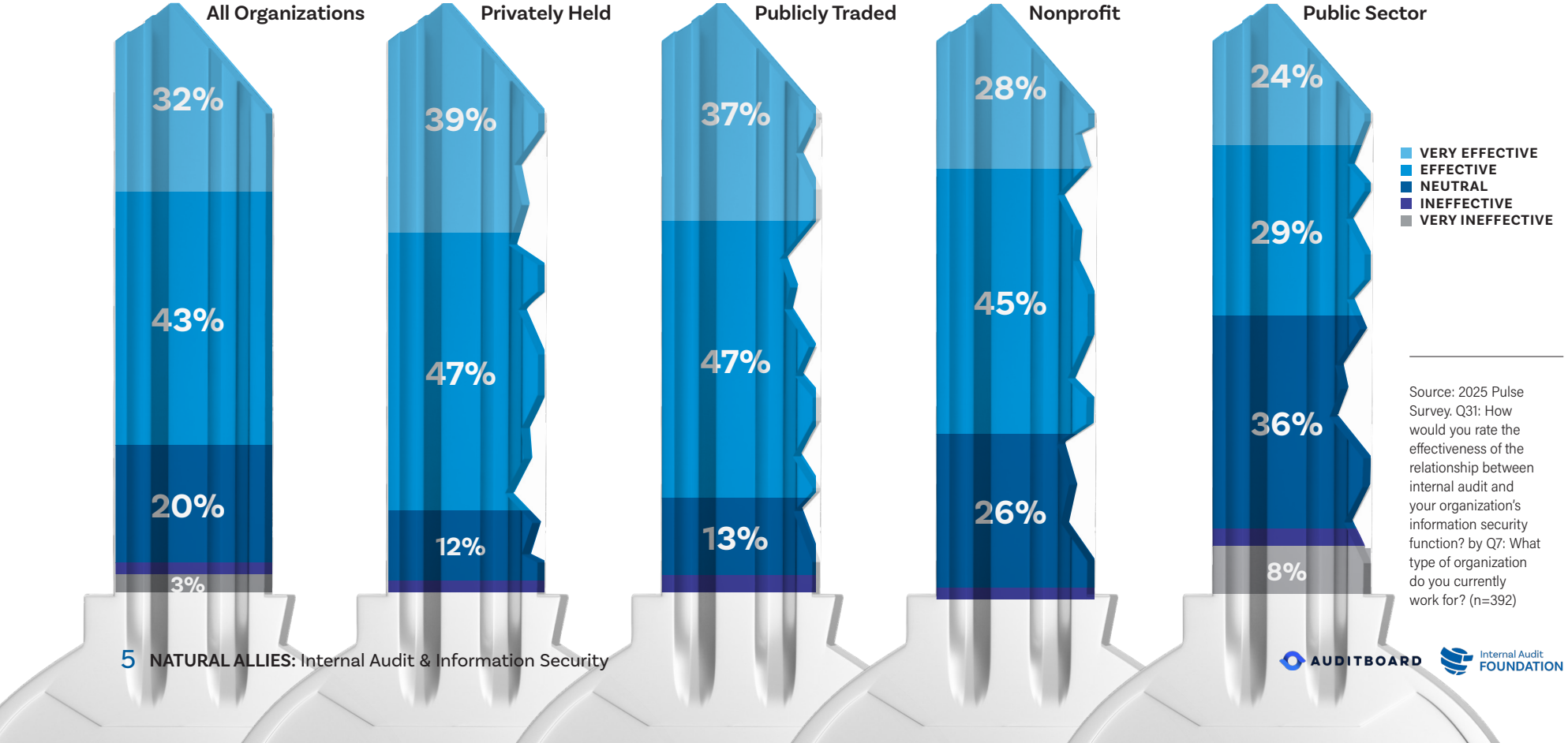
"It was nice to kind of glide in and interact with her from the start," he said. "We can have those discussions and parse out what each different team is responsible for so we're not overlapping."

The benefits of collaboration can quickly become apparent in newly established internal audit-information security relationships, as well. For example, an internal audit leader from a U.S. city described how a cyber incident brought together internal audit and information security. "Sometimes pain brings people together," she said. "I think they're seeing now why it's important for us to work together."

That now includes internal audit working to identify new software to support information security, she said.

FIGURE 3

Relationship Effectiveness & Organization Type



Source: 2025 Pulse Survey. Q31: How would you rate the effectiveness of the relationship between internal audit and your organization's information security function? by Q7: What type of organization do you currently work for? (n=392)

AUDITBOARD Internal Audit FOUNDATION

Younger audit leaders meet more frequently. The second deviation finds a generational difference, with older internal audit leaders meeting less frequently with information security professionals. Internal audit leaders from the Baby Boomer generation (1946 to 1964) are more likely to meet annually or quarterly than monthly with their information security counterparts. In contrast, audit leaders from the Gen X (1965 to 1980) and Millennial (1981 to 1996) generations are more likely to meet monthly or more than once a month (see Figure 4).

Mature Benefits Are Harder to Achieve

Participants in the 2025 Pulse survey were invited to share insights into the tactical approaches they employed to strengthen the working relationship between internal audit and their organization's information security function. Among those who rated the effectiveness of the relationship as high (i.e., very effective or effective), over 140 individuals provided feedback to this open-ended question. Their qualitative responses were analyzed to identify recurring patterns, which were then aggregated to develop overarching themes.

The analysis of the written responses revealed that while many participants emphasized the importance of communication, visibility, joint involvement, collaboration, and efforts to build relationships as key factors for fostering effective relationships between internal audit and information security, more advanced approaches — such as establishing credibility and trust through delivered services — were mentioned less frequently (see Figure 5).

FIGURE 4

Generation & Meeting Frequency

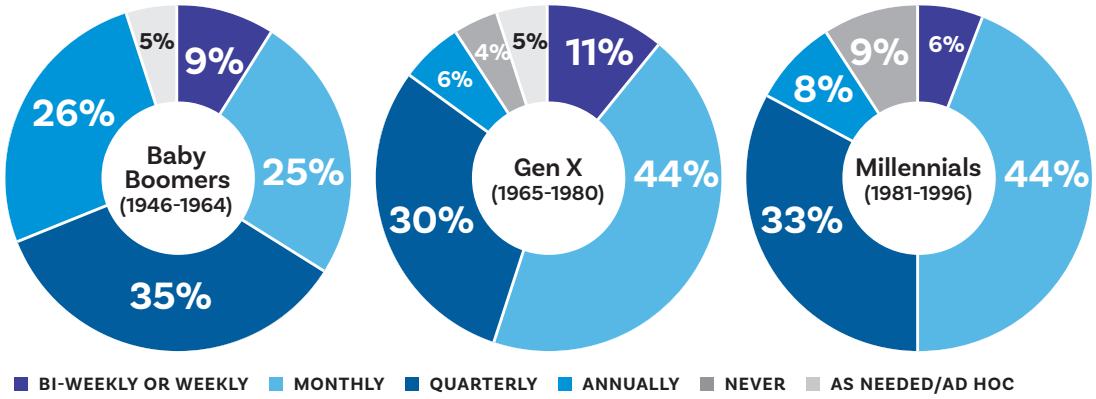


FIGURE 5

Tactical Approaches for Effective Relationships

62% Communicating regularly

22% Aligning on projects and goals; collaborating to solve issues

18% Building relationships

17% Gaining visibility and encouraging joint involvement

6% Establishing credibility and gaining trust through services

Figure 4, Source: 2025 Pulse Survey. Q30. How frequently does internal audit meet with your organization's information security function to discuss security issues? by Q57: Please select your year of birth. (n=382)

Figure 5, Source: 2025 Pulse Survey. Q32. What tactical approaches have you used to develop a strong working relationship between internal audit and your organization's information security function (optional)? (n=143)

Five Emergent Themes

Tasks or actions identified as beneficial for strengthening internal audit–information security relationships, along with sample insights

#1

Communicating regularly—whether weekly, monthly, quarterly, or as needed

"We still talk regularly, even if it's not official."

"Almost daily interaction with CIO, CISO, and their staff by Internal Audit Director and IT Auditor."

#2

Aligning on projects and goals, and collaborating to solve issues

"We've found that we both have a common goal of reducing risk to the enterprise, so that's helped."

"We have an aligned assurance approach where Internal Audit, Compliance, and InfoSec meet regularly and stay aligned with their initiatives and plans, and try to make sure we are taking a comprehensive [approach]."

#3

Building relationships

"Build a solid working relationship to try and understand technology."

"Honest conversation and collaborative attitude to improve information security."

"Attending conferences jointly with them to learn and build relationships."

#4

Gaining visibility through board and/or committee memberships, and encouraging joint involvement/inclusivity

"We sit on the security committee and provide feedback in real time to IT risk decisions."

"Joint board updates."

#5

Establishing credibility and gaining trust through services

"They also view our work as high quality and seek our assistance on assessment matters."

"Fair and objective audit work, but also standing our ground."

"Advisory services to gain trust."

Benefits of Collaboration

Similar to the Pulse survey participants, the internal audit and information security leaders who took part in the roundtable discussions cited numerous benefits of collaboration. These benefits included coordinated risk assessments, improved communications with the board, and combined assurance efforts. As advances in technology boost business competition and the need for efficient operations, these benefits take on greater value. The following sections provide more in-depth exploration of the insights gathered from the roundtable discussions.

Alignment

Alignment on cyber-related risks helps internal audit focus on assurance that provides relevant and immediate value to information security. An internal audit leader from the hospitality and tourism industry shared how he leverages comprehensive risk assessments developed by the organization's information security team.

"These are the risks that drive what projects we're going to be focused on in the coming year," he explained. "We align and collaborate with information security and our chief information officer on where our time is best spent from a project perspective in supporting them and their ultimate goals and objectives."

The public sector CISO said coordinating and aligning work calendars also supports his long-term planning. "She has her calendar of events and a certain number of internal audits she has to do. And I have my calendar of events," he said. "By working together and aligning what she's doing, she's structuring her audits in a way that I'm getting information that I need to feed into my future planning."

Alignment on messaging to the board offers clear and accurate assessments of the organization's cybersecurity profile and can help avoid embarrassing conflicts. A vice president of internal audit and risk

management within the financial services industry recalled how internal audit's collaboration with information security evolved to improve communication with the board.

"At first, we weren't necessarily communicating a lot with the board regarding information security," he said, while acknowledging that today's regulations demand greater engagement. "So, it was internal audit that pushed back to information security saying, 'Look, we have to give the board more information than you're giving them currently.' That has tremendously improved."

Speaking a single truth to the board about an organization's cybersecurity status helps prevent confusion and potential conflicts that can create inefficiency and sow doubt. The roundtable participants frequently cited collaboration on messaging and sharing presentations as effective strategies.

"What I've found helpful is to share my presentations with the CISO, just so they know what I'm telling the audit committee, and conversely, they share what they're briefing the board and the audit committee about," said the audit leader of an information and analytics company.

He recalled an incident where his CISO told board members all was well on the cyber front the day after he briefed the board about numerous internal audit findings relating to cybersecurity.

"The board said, 'Wait a second. This guy just came in and said all this stuff.' So, he had to backpedal a little bit. He was giving macro level assurances. If we have a few findings here and there, it doesn't mean the house is on fire. So that was a lesson learned; Collaborate and share those materials the best that you can."

The risk and audit leader at the public transit authority said she routinely invites her CISO to speak at executive risk management committee meetings not only to coordinate board messaging, but also to stay informed on information security risk management efforts.

"That allows us to stay connected in preparation for the [board] meeting as well as being able to speak in terms of things that they're doing and things that we're able to validate on our end," she said.

Her CISO added that the board receives quarterly information security reports that are clear and accurate.

"I know what she's briefing, and she knows what I'm briefing. We're keeping that kind of messaging to the board consistent, and they're not getting conflicting information," he said. "That clear and consistent messaging also provides a level of confidence to the board and executive leadership that we are collaborating, and things are moving in the right direction."

Coordination

Coordination between internal audit and information security on compliance efforts, use of cybersecurity frameworks, joint use of technology, and risk management assurance provide

> "By working together and aligning what she's doing, she's structuring her audits in a way that I'm getting information that I need to feed into my future planning."
>
> —Chief Information Security Officer

additional avenues for improving an organization's cybersecurity.

Internal audit assurance supports regulatory compliance in multiple ways. The public transit CISO said the aligned assurance work cited earlier also supports compliance with federal rules on independent verification and validation, commonly referred to as IV&V.

"You have your cybersecurity function, and you have your IV&V team, which is independent of the cybersecurity function and checks the work," he said. "I don't have enough staff to have an IV&V team, so [internal audit's] team fills that function for me. I get a free service from her team that provides me value — and in addition to that, I get the feedback on work that we've done over the year, validation that the work is done to standard, and that we can close some of those findings."

Internal audit findings also help identify areas that need work, so it provides support for planning, he said. "It's a to-do list for my next two or three to four years of planning," the CISO said. "We're making sure that we're talking and aligning what we're doing, and she's maintaining that independence because, you know, she's certainly not here to just give me a free pass."

The organization's audit leader agreed. "When we're looking at significant systems and [Information Security] has identified the top five systems, they may look at two of them, we might consider the other three during our audit planning," she said. "So, we're able to provide full coverage on what we collectively believe to be significant systems in the organization for any given year."

An added benefit of having an established relationship is the ability to jointly strategize on how best to show compliance with regulations that can be complex and arduous.

"We have to figure out how to come up with accurate, meaningful answers to high-level questions and be able to defend [them] when somebody comes in to challenge us," the CISO said. "That's going to take a lot of cross-talk between our different teams to look at the data and figure out how to win it."

Collaboration can help mitigate risks of cyber incidents and related reputational risks. An audit leader within the healthcare industry noted that not only does collaboration support regulatory compliance, but regulations and cyber incidents can drive collaboration, as well.

"If one employee gets hit and that employee has 1,000 patient records that get exposed to the threat actor, not only are you required to report that to OCR, but you also get put on their wall of shame," he said, referencing the U.S. Department of Health and Human Services Office for Civil Rights. "You also are required to notify press, radio, or TV in your market. So, the stakes are huge. In healthcare that trusting relationship means everything."

> "I get a free service from her team that provides me value."
>
> —Chief Information Security Officer for major metropolitan transit authority

Coordination will be critical to effective and safe use of artificial intelligence (AI). Collaboration on risk assessments, shared technology tools, and transparent communications set the foundation for effectively managing new technology and cyber risks, such as artificial intelligence.

The public transit risk and audit leader stated that her function's involvement in cybersecurity governance exercises in an

advisory capacity gives them a seat at the table for discussions on evolving technology risks.

"As new issues come about, we continue to stay connected," she said. "So, I think one recent thing for us is looking at the AI space. Whether it's in terms of acceptable use policies and how it helps data organization from a testing standpoint or from an interest standpoint, we at least have conversations there."

Education and Advocacy

Speaking information security's language is critical to acceptance and trust. The risk management and internal audit leader from the financial services industry stated that his knowledge of information security was critical in establishing a strong working relationship when he first took on the job.

"When I first showed up, being able to talk their language really went a long way to developing that collaboration between us and the information security group and our technology group," he said.

He remains a strong advocate for internal auditors to become educated enough about information security to speak knowledgeably about their needs.

Internal audit can act as a strategic advisor and advocate on information security's behalf. The U.S. city audit leader's evolving relationship with her information security team has paid an unexpected dividend. Internal audit was able to articulate information security resource needs more effectively to executive management.

"I think for quite a while, they felt like what they were saying they needed was falling on deaf ears," she said, adding that there was resistance to information security requests for additional software until internal audit was able to convince budget-conscious administrators of the need.

"Now we're looking at five different software programs, and they've been approved for all five of them," she added. "In years past, they hadn't been because there wasn't a good intermediary there to bring to the city manager's attention that it was necessary."

The key, she explained, was having internal audit demonstrate that the new software would enhance productivity and be far more cost-effective than hiring additional staff. She also emphasized that building a trusting relationship was critical to having information security share their needs.

An audit leader in the food manufacturing industry shared a similar observation. Her organization is going through an ownership change, which also involves a shift in culture. Part of this transition includes conforming to additional reporting requirements for the privately owned company.

> "If one employee gets hit and that employee has 1,000 patient records that get exposed to the threat actor, not only are you required to report that to OCR, but you also get put on their wall of shame."
>
> —Audit, Risk, and Compliance Leader

"It has been a challenge for both InfoSec and our group to demonstrate upward the need for additional resources and additional processes," she said. "So, we've been collaborating on presentations to explain the difference between the execution steps and the compliance steps and the need for all the different things coming into that."

Sharing Technology

Internal audit and information security can leverage GRC tools to enhance transparency and strengthen collaboration. Governance, risk, and control (GRC) software is a rapidly growing business market with a variety of products available, from off-the-shelf tools to highly specialized systems designed for specific users. As new cyber threats emerge and new risk management strategies and regulations evolve to better manage those risks, it is safe to say that GRC technologies will play a greater role. While GRC tools undoubtedly are an important component of cybersecurity, collaboration on the use of those tools holds even greater promise.

The public transit agency CISO said information security and internal audit share the same GRC technology.

The shared technology provides internal audit with visibility into what information security is doing, which provides benefits on several levels, including knowing what process and systems reviews information security has done and avoiding duplication.

The chief risk and audit officer at the agency added, "We're looking somewhat in that space of combined assurance so we're not duplicating and are complementary."

IIA Global Technology Audit Guides (GTAGs)

The following guides are available for free to IIA members and offer support for conducting internal audit activities:

- Assessing Cybersecurity Risk: The Three Lines Model
- Auditing Business Applications

UPDATED!

- Auditing Cyber Incident Response and Recovery, 2nd Edition
- Auditing Cybersecurity Operations: Prevention and Detection

UPDATED!

- Auditing Identity and Access Management, 2nd Edition
- Auditing Insider Threat Programs
- Auditing IT Governance (Previously GTAG 17)

UPDATED!

- Auditing Mobile Computing, 2nd Edition

UPDATED!

- Auditing Network and Communications Management, 2nd Edition
- IT Change Management: Critical for Organizational Success, 3rd Edition (Previously GTAG 2)
- IT Essentials for Internal Auditors
- Understanding and Auditing Big Data

BUILDING EFFECTIVE RELATIONSHIPS:

Strategies and Goals

The open-ended feedback collected through the Pulse survey, along with the insights gathered from internal audit and information security leaders at the two roundtables, identified various strategies for establishing and strengthening the relationship between internal audit and information security.

Meet often.

Meeting cadence is associated with successful relationships. Simply put, more communication, both formal and informal, leads to more effective relationships.

Create committees of relevant technology and audit leaders.

Several participants in the roundtables identified the creation of specific committees within their organizations that brought together key players from information security, compliance, information technology, and internal audit.

Build cybersecurity into all internal audit engagements.

Keeping cybersecurity top of mind in every audit engagement supports holistic approaches to risk management. Additionally, strong internal audit-information security relationships help ensure that engagements provide relevant, useful, and timely assurance.

Look for ways to share technology tools, frameworks, and software.

Effective collaboration builds trust between internal audit and information security, which can lead to greater transparency and information sharing. The public transit agency CISO acknowledged that overcoming resistance to data sharing can be a challenge.

"We tend to be very, very secretive with our data, especially when it comes to vulnerability data for specific systems," he said. "There's a huge level of trust knowing [the internal audit] team and knowing I can share that data with them."

The maturity of that relationship now includes shared technology that provides internal audit with greater access to certain data.

"We put it all in one system, and they're only going to use it for the purposes they need for enterprise reporting," he said. "So, we can have that kind of information sharing without elevating the risk profile of too many people."

The care for data security is reciprocal. The public transit risk and audit leader said information sharing within their shared GRC platform is role-based, so that some data is only available to her in her capacity as chief audit executive.

"I'm making sure that people understand that our goal with information sharing is making sure confidentiality is respected," she said. "I think it's helpful to say on the front end, 'Hey, I'm getting this from you, but it's going to be limited to XYZ at this point.' I think that kind of assurance is comforting."

Look for opportunities to align risk assessments, assurance, and information sharing.

As noted in previously cited examples, aligning risk assessments, assurance reviews, and audits helps to avoid unnecessary duplication of effort. This is particularly valuable considering resource limitations.

"It's really competing priorities and limited capacity," one internal audit leader observed. "There's so much more that we could be providing assurance and advice and insight on than what we already are. We just sort of have to pick and choose what's the biggest bang for the buck."

Coordinate messaging to the board.

Clear and consistent messaging to the board, particularly regarding an organization's cybersecurity status, helps prevent confusion, avoid potential conflicts, and improve efficiency.

Create opportunities to share knowledge.

Guest auditor programs, reciprocal training, and debriefings support coordination and collaboration. The audit leader from the information and analytics company said their guest auditor program includes employees from various areas of the organization, but those that involve information security are the most valuable.

"I think we get the most bang for our buck with InfoSec," he said. "If we're doing a cybersecurity audit, we will take someone from the InfoSec team to help audit another business. We get their deeper technical skills because I think as auditors, we can only be so technical since we're not actually performing the controls."

The benefit to information security is that their employees learn how other parts of the organization are implementing and operating technology. This leader's organization also provides internal audit employees through a secondment program. Internal audit benefits when analysts develop new skill sets, build new relationships, and gain a greater understanding of the inner workings of the company.

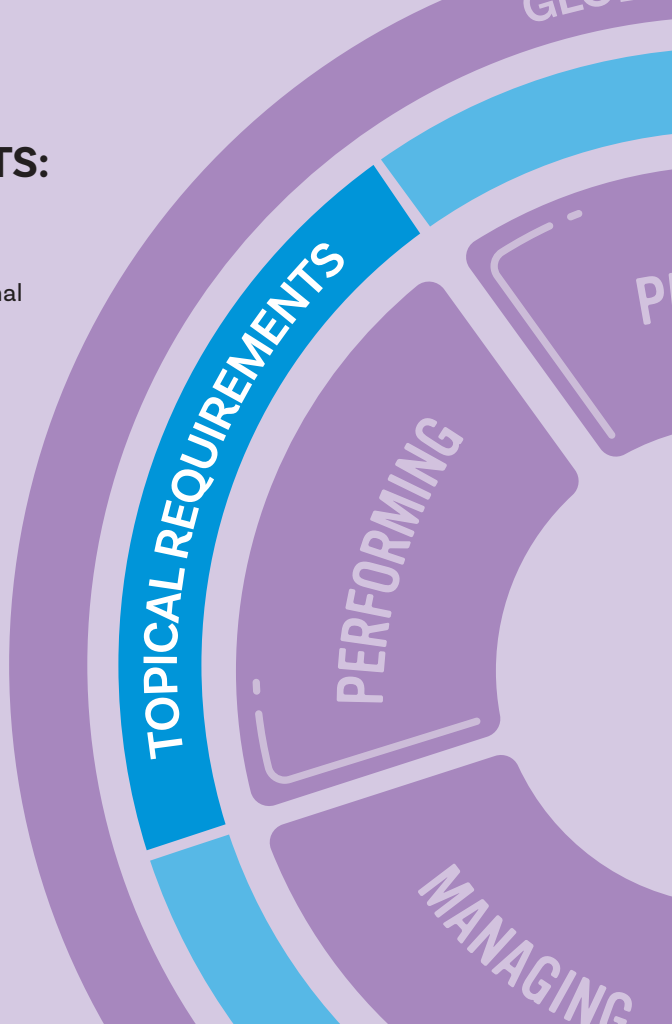
Another avenue for information sharing is shared training. "We [in internal audit] go to training events, information security goes to training events, and we share some of that information, tips, and tricks," said an audit leader from the health insurance industry. "I think it helps build respect for one another, that we're knowledgeable in our fields and can bring value to each other."

TOPICAL REQUIREMENTS: CYBERSECURITY

Topical Requirements are a mandatory component of the International Professional Practices Framework® (IPPF®). By adhering to these requirements, internal audit functions, regardless of their size, ensure the consistent application of audit methodologies in a specific topical area.

Cybersecurity is one such topical area. When performing an internal audit engagement that includes cybersecurity objectives in its scope, internal auditors must assess whether the organization's governance, risk management, and control processes adequately address cybersecurity risks.

For guidance on assessing the necessary aspects of cybersecurity processes, please refer to theiia.org/TopicalRequirements.



Supporting Cyber Resilient Cultures

Cyber incidents often spark greater awareness of vulnerabilities and can be catalysts for strengthening overall cyber resilience. As noted by more than one roundtable participant, cyber incidents can also motivate greater cooperation and collaboration between internal audit and information security. But it doesn't have to be that way.

Effective internal audit-information security relationships can support efforts to build cyber resilient organizations without having to go through the pain of a cyberattack. As natural allies on the cyber battlefield, internal audit and information security can team up to communicate the need and value of a healthy cyber culture.

"I've been doing this for well over two decades now, and one tends to get a lot of pushback when you tell people they have to patch their systems because they're busy and they have a lot of other things to do," the public transit CISO said. "Having another person in the organization be able to highlight those risks at an enterprise level helps me a lot."

The audit leader of a U.S. city shared that a cyber incident served as the catalyst for increased internal audit involvement in information security. But it also sparked greater collaboration on cybersecurity throughout the organization.

"Since the cyber event, we meet on a weekly basis now with our IT team surrounding cybersecurity," she said. "That's the only topic that we talk about in this meeting because we want to build resiliency across every department."

The meetings now include the CISO as well as representatives from internal audit who are ready to provide cybersecurity training for other departments.

"It's not just directors," she said. "We're going to have the managers do tabletops with the actual staff that touch the computers and the different devices on a daily basis."

The audit leader from the financial services industry said his relationship with information security now includes providing assurance on mandated disaster recovery and incident response exercises previously provided by outside consultants.

"Our internal audit function is sitting in on those tabletop activities and assessing them and providing that objective report to our Board of Directors and to our regulatory authorities," he said.

Any discussion about cyber resilience should include a list of key steps, including identifying assets, developing policies and procedures, implementing security controls, monitoring activity regularly, training employees, testing systems regularly, and having an incident response plan in place.[8]

Internal audit should provide assurance over each step, but this doesn't mean others can't. Second line functions, including information security, can do so as well, and effective relationships between internal audit and information security make aligning assurance over those key areas easier.

8 "What Is Cyber Resilience and Why Does It Matter?", Synack, accessed December 16, 2024.

Information Security Resources

CYBER RESILIENCE REVIEW (CRR)
Self-assessment methodology developed by the U.S. Cybersecurity and Information Security Agency (CISA) that measures an organization's cyber resilience capabilities.

ISO/IEC 27001
An international standard for information security management systems (ISMS).

NIST CYBERSECURITY FRAMEWORK
Developed by the U.S. National Institute of Standards and Technology (NIST), this framework provides cybersecurity guidance focused on small-to-medium sized businesses.

Overcoming Challenges

Building effective internal audit-information security relationships can seem daunting. Commitment to conquering resistance, breaking down silos, educating key participants, and creating opportunities for information sharing is difficult, particularly when audit and information security leaders are battling limited time and resources. However, the benefits can be significant. A fundamental part of successful relationships is building trust and recognizing the value each side brings to the table.

Understanding Internal Audit's Value

A variety of real-world examples of collaboration and cooperation have been shared that reflect how greater interaction can lead to greater appreciation. For the U.S. city audit leader, that appreciation was born from the two sides being thrust into responding to a cyber event. However, such trauma isn't required.

Indeed, the audit leader said a pivotal change involved hiring a new chief information officer (CIO) who had previous experience as an IT internal auditor.

"It really helped bridge that gap of understanding the importance of internal audit and looking at those risks from a different viewpoint," she said, adding that he has helped communicate internal audit's commitment to confidentiality.

"We want to be very careful and mindful of what they're doing," she said. "But at the same time, we want to help them to increase their ability to be more resilient."

Formalizing the relationship opens doors to greater involvement by internal audit in strategic advisor roles, said one audit leader.

"We are implementing a major, financially significant system, and we're taking a much more structured approach to participating in those projects, consulting on the control aspects, and helping them think about efficiencies," he said.

Breaking Down Silos

Information security, by definition, is focused on keeping information secure, which can lead to resistance to sharing information. Information security and internal audit leaders speaking at the roundtables acknowledge there are plenty of good reasons to be stingy with information — cybersecurity, data privacy, regulatory compliance, competition. However, the benefits to coordinated risk management and combined assurance easily outweigh risks associated with judicious information sharing.

The mutual trust developed by the CISO and audit leader at the public transit organization reflect how mature relationships can lead to effective, productive information sharing.

Alignment and Transparency

The complexity of today's cyber risks demands that organizations seize every opportunity to minimize those risks. Aligning on risk assessments, planning, combined assurance, compliance efforts, and emerging technologies such as generative artificial intelligence all contribute to strengthening an organization's cybersecurity profile.

Conclusion

Practices that strengthen cybersecurity and help grow cyber resilient organizations should be examined and embraced. Conversely, practices that endorse hoarding information and building silos will ultimately lead to cybersecurity failures.

The list of benefits to effective internal audit-information security relationships is long (see Figure 6), and any risks that are associated with sharing information with internal audit can be easily overcome through policies and processes that ensure data remains protected.

While not all organizations enjoy the benefits of formal information security and internal audit functions, those that do would be well served by nurturing a collaborative relationship between them.

FIGURE 6

Qualities of Effective Internal Audit-Information Security Relationships

	INTERNAL AUDIT PROCESSES	COLLABORATION BENEFITS	STRATEGIES	CYBER RESILIENT CULTURE
Cybersecurity built into all audits.	🔒		🔒	
Improved Internal Audit knowledge of InfoSec.		🔒		
Cyber incidents fuel collaboration.				🔒
Joint risk committees created to improve collaboration.		🔒		
Breaks down silos.		🔒		🔒
Supports combined assurance.	🔒	🔒		
Joint use of technology tools/software.		🔒	🔒	
Encourages alignment/transparency.		🔒	🔒	
Collaboration on AI adoption/use.		🔒	🔒	🔒
Improves data sharing/information flow.	🔒	🔒		
Enhances Internal Audit value recognition by InfoSec.		🔒		
Coordinates board communications.		🔒	🔒	🔒
Supports cybersecurity messaging to the organization.		🔒	🔒	🔒
Supports regulatory compliance.		🔒		🔒
Identifies emerging risks/trends.		🔒		🔒
Positions Internal Audit as InfoSec advocate.		🔒		🔒
Enables greater transparency in audit engagements.	🔒		🔒	
Focuses reputational risk considerations.		🔒		🔒
Reciprocal training/guest auditor.	🔒		🔒	
Positions Internal Audit as strategic advisor.	🔒	🔒		

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, compliance, and ESG management. More than 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.

About The Institute of Internal Auditors and the Internal Audit Foundation

The Institute of Internal Auditors (The IIA) is an international professional association that serves more than 255,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. **For more information, visit theiia.org.**

The Internal Audit Foundation is an essential global resource for advancing the internal audit profession. Foundation-funded research provides internal audit practitioners and their stakeholders with insight on emerging topics and promotes and advances the value of the internal audit profession globally. In addition, through its Academic Fund, the Foundation supports the profession's future by providing grants to students and educators who participate in The IIA's Internal Auditing Education Partnership program. **For more information, visit theiia.org/Foundation**.

AUDITBOARD Internal Audit FOUNDATION


AUDITBOARD
Internal Audit
FOUNDATION