Internal Audit and AI-enabled Fraud

AuditBoard

Internal Audit FOUNDATION
1976-2026

Table of contents

Executive summary

Artificial intelligence (AI) is rapidly reshaping organizational operations, enabling new levels of efficiency, automation, and insight across core business processes. These same capabilities, however, enable new fraud techniques and enhance the scale, speed, and effectiveness of traditional fraud methods. AI-enabled tools can generate highly convincing phishing schemes by fabricating financial documentation, manipulating audio and video evidence, and producing hyper-personalized communications designed to evade traditional controls. As organizations rapidly integrate AI into their operations, responsibility for understanding, assessing, and responding to these emerging fraud risks increasingly falls within the purview of internal audit, creating a critical imperative for the function to adapt to this evolving risk landscape.

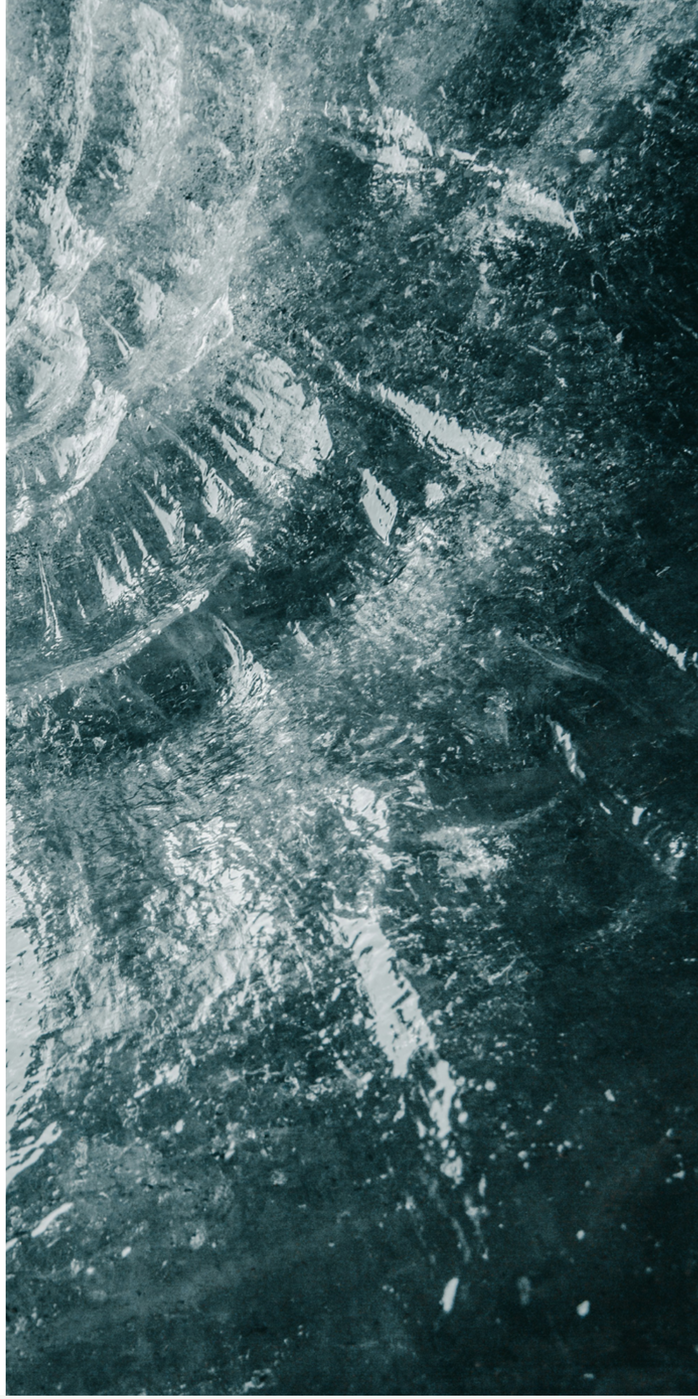
The Internal Audit Foundation, in partnership with AuditBoard, surveyed 373 senior internal audit leaders to understand how audit functions currently perceive AI-enabled fraud risk, their preparedness to address it, the barriers to an effective response, and the most important actions to take now.

Insights indicate growing vigilance of AI-enabled fraud, but uneven familiarity and limited confidence in readiness. While 85% of respondents view AI-enabled fraud as a moderate to high risk, fewer than four in 10 believe their internal audit functions remain adequately prepared to detect it. Familiarity with AI-enabled fraud is associated with higher perceived risk, suggesting that a deeper understanding of AI-enabled fraud contributes to greater awareness of exposure rather than reassurance. Concern seems to be focused on more visible threats, such as AI-powered phishing, while rapidly expanding risks, like synthetic identity fraud, remain less widely recognized.

Persistent barriers hamper preparedness in the form of:

- Limited access to appropriate tools
- Insufficient skills and expertise
- Budgetary constraints
- Competing organizational priorities

At the same time, internal audit's use of AI is increasing, and most respondents expect that trend to continue in the near term. This growing familiarity presents an opportunity for the internal audit team to strengthen its ability to identify misuse, assess controls, and advise management more effectively.



Introduction

Over the past decade, rapid technological advancements in AI have profoundly reshaped many aspects of modern life. AI has quickly embedded itself in the home, the workplace, and third places where people gather and connect. This integration is fundamentally reshaping daily routines, expanding productivity, and driving the demand for new skills.

AI tools are increasingly integrated into legacy business processes, accelerating workflows, automating routine tasks, and assisting in our work. A 2024 McKinsey study found that 78% of respondents report AI adoption in at least one business function, up from 50% in 2022.[1]

AI can expand human capabilities and democratize access to knowledge and skills. However, far less attention is paid to its potential misuse as both a powerful enabler of novel fraud techniques and a magnifier of the speed, scale, and success of traditional fraud schemes. Widely available systems, such as OpenAI's Sora and DALL-E, Google's Imagen, and Adobe's Firefly, produce lifelike images, videos, and audio, which bad actors can exploit at scale to generate fake documentation and manipulate evidence that organizations rely on and internal auditors review in audit engagements. To manage AI risks effectively, organizations must establish processes to detect and deter misuse. Internal audit plays a key role by providing strategic guidance over those efforts.

Globally, fraud is increasing. A 2022 LexisNexis report focusing on financial institutions, retail, and e-commerce noted that, while legitimate transaction volume rose 15% year over year, human-initiated fraud attempts climbed 19%.[2] In 2025, the World Economic Forum's Annual Meeting focused on the rise of cybercrime, particularly identity theft and fraud. In 2023 alone, the use of AI-generated deepfakes to circumvent identity verification increased by a shocking 704%.[3] This growth suggests that AI technologies are enhancing the sophistication, automation, and effectiveness of fraudulent activities designed to evade existing controls. To better understand how rapid advancements are reshaping the threat landscape, it is important first to consider what AI is and how it operates.

"Company worker in Hong Kong pays out £20 million in deepfake video call scam."

THE GUARDIAN

"U.S. Federal Bureau of Investigation (FBI) warns of increasing threat of cyber criminals utilizing artificial intelligence."

FBI SAN FRANCISCO MEDIA OFFICE

"Italian police freeze cash from AI-voice scam that targeted business leaders."

REUTERS

Key terms and definitions

The Institute of Internal Auditors (The IIA) in the Global Internal Audit Standards™ defines "fraud" as "an intentional act characterized by deceit, concealment, dishonesty, misappropriation of assets or information, forgery, or violation of trust perpetrated by individuals or organizations to secure unjust or illegal personal or business advantage." [4] For consistency, this report uses the term "AI-enabled fraud" to describe both novel schemes supported by AI tools, as well as more traditional schemes enhanced by AI.

AI encompasses a family of technologies underpinning a suite of applications and platforms, defined as "an engineered or machine-based system that can, for a given set of human-defined objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments".[5] While the application of AI is broad, this study focuses specifically on those AI systems most likely to be leveraged to enable fraud. Though extant literature does not provide a validated hierarchy, a brief review of the AI-enabled fraud landscape finds three types are most prevalent:

1. **Generative AI (genAI):** computational techniques capable of generating seemingly new, meaningful content, such as text, images, or audio, from training data[6]
2. **Agentic AI:** autonomous, goal-driven systems that can operate for long periods, requiring minimal human supervision[7]
3. **Conversational AI:** software agents that can engage in natural conversational interactions with humans[8]

The IIA and Internal Audit Foundation (Foundation) have examined how organizations and internal audit functions use AI and other digital systems. Data from the Foundation's Risk in Focus 2026 Global Summary report shows that digital disruption, including AI, has steadily increased as a top five risk, year over year, based on risk rankings by senior internal audit leaders. Since 2023, digital disruption has increased by 14%, making it the fastest-growing risk over the last three years.[9] Furthermore, the Foundation's 2025 North American Pulse of Internal Audit found that 41% of internal audit leaders were currently using genAI for internal audit activities, with 65% planning to increase genAI involvement.[10] This provides a reliable, quantifiable measure of how quickly digital technology is changing the risk landscape.

This report offers a deeper look into organizational familiarity with, experience in, and use of AI, as well as preparedness for AI-enabled fraud. It draws on a diverse range of internal audit functions to provide a benchmark across industry, sector, and size. Organizational preparedness varies: some organizations boast codified policies and dedicated resources to address the risk posed by this type of fraud. In contrast, others report far less capability to address this emergent risk area. Regardless of size, sector, maturity, or familiarity, this report sheds light on the ongoing conversation about the new risks and opportunities posed by the evolution of this technology.

The phantom vendor scheme

While we often treat the three AI technologies — generative, agentic, and conversational — as separate tools, they can be combined to carry out sustained, scalable, and highly personalized fraud.

For example, an attacker could analyze vendor payment records to identify payment cycles and past transaction patterns, then feed those signals into a large language model to produce a prioritized list of times and departments most likely to approve invoices without additional review.

The attacker could then use generative AI to create a synthetic vendor identity and AI-generated invoices that mimic authentic vendor formats and line-item details. Finally, a conversational AI agent could interact directly with accounts payable, answering follow-up questions instantly and convincingly, even referencing legitimate past transactions to build trust and push the fraudulent payments through.

Methodology

In Q4 2025, the Foundation and AuditBoard distributed an online survey to North American internal audit leaders to assess current awareness and practices related to AI-enabled fraud. Survey questions focused on five key subjects:

Familiarity

How familiar are internal audit functions with the risks posed by AI as it relates to fraud, and how do they rate the potential impact within their organizations?

Experience

Have organizations encountered instances of AI-enabled fraud, what was the nature of those incidents, and what was the extent of internal audit's involvement in analyzing them?

Use of AI

How do internal audit functions currently use AI tools, and what are their plans for future adoption?

Preparedness

How do internal audit functions perceive organizational preparedness with respect to AI-enabled fraud risks, what actions are they taking, and what barriers do they face in developing effective responses?

Response

How have internal audit functions responded to AI-enabled fraud risks, what actions are they taking, and what roles are they playing within their organization?

A total of 373 individuals from all sizes of internal audit functions and organizations, across diverse industries and sectors, completed the survey. Respondent demographics are included in the appendix of this report.

The IIA's Artificial Intelligence Knowledge Center

Artificial intelligence is being adopted at a rapid pace across the enterprise. The IIA has created an entire knowledge center focused on providing a variety of resources on the topic. To access The IIA's Artificial Intelligence Auditing Framework, learning resources, podcasts, and videos focused on artificial intelligence, scan:

Findings

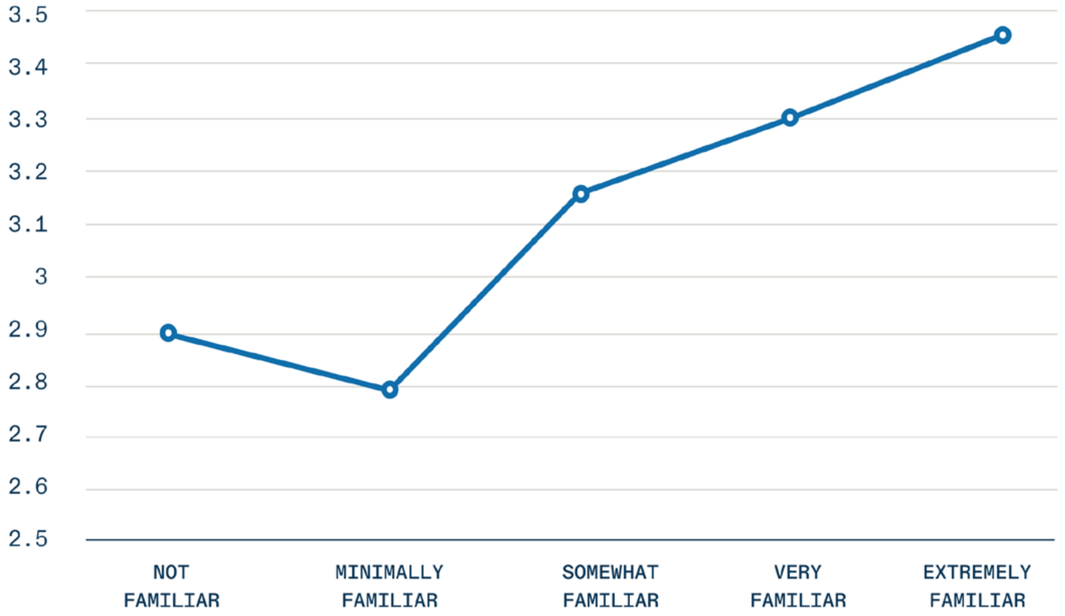
Risk perception rises with familiarity

More than half (51%) of senior internal audit leaders are somewhat familiar with the concept of AI-enabled fraud, with fewer (34%) reporting they are very or extremely familiar, and a smaller group (15%) stating that they have minimal or no familiarity with the risk. Variance exists in how individuals perceive this risk, with a majority (58%) seeing it as a moderate risk, a little more than a quarter (27%) perceiving the risk as high or very high, and fewer than two in 10 (15%) seeing it as a low or very low risk. Analysis of cross-tabulated results finds several significant ($p<.05$) differences between familiarity and perceived risk levels.

To examine this relationship, numeric values were assigned to the Likert scale responses for Q14, "How would you describe the level of risk for AI-enabled fraud at your organization?", with 1 corresponding to "very low risk" and 5 corresponding to "very high risk." This scoring enabled the calculation of mean perceived risk scores across different levels of familiarity with AI-enabled fraud, shown in Figure 1. Respondents who reported no familiarity with AI-enabled fraud had a mean perceived risk score of 2.9. Interestingly, those reporting minimal familiarity had a slightly lower mean score of 2.8, which is expected when considering the impact uncertainty has on how risk is perceived. This dip is followed by a steady increase in perceived risk as familiarity grows, with respondents who reported being very or extremely familiar with AI-enabled fraud registering the highest perceived risk score of 3.4 out of 5.

FIGURE 1

Mean perceived risk score by familiarity



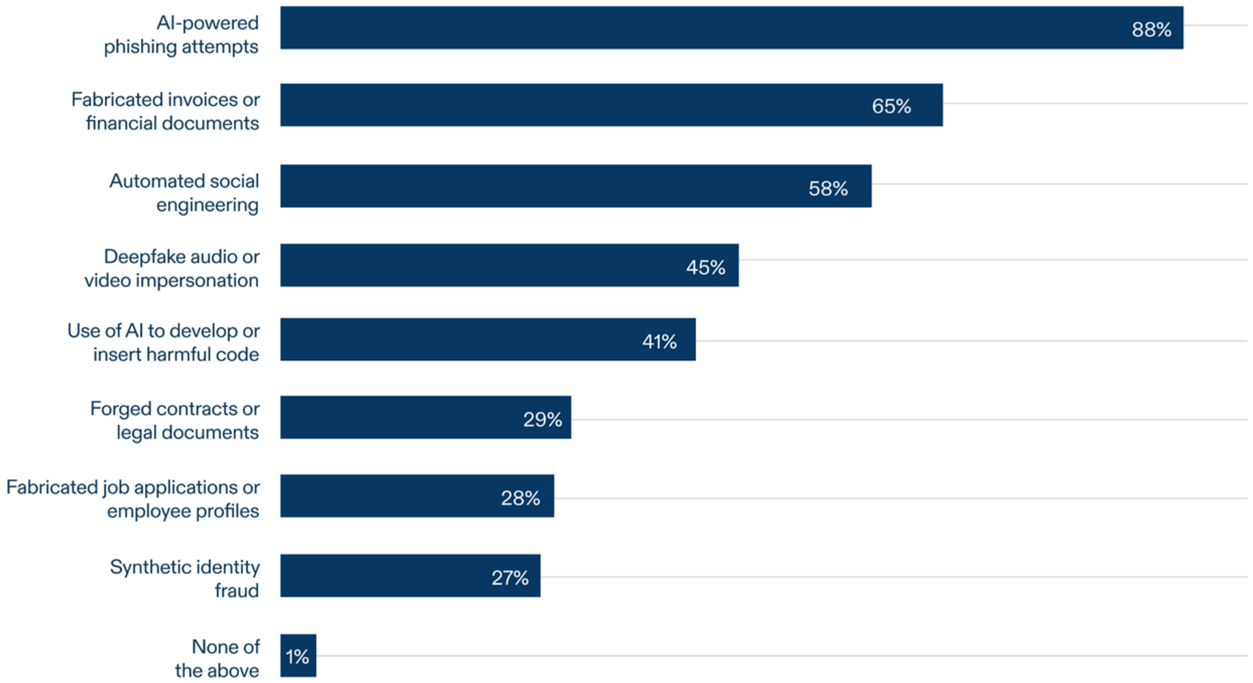
Q13: How familiar are you with the concept of AI-enabled fraud? (n=373)
by Q 14: How would you describe the level of risk for AI-enabled fraud at your organization? (1 very low to 5 very high)

Organizational concerns for AI-enabled fraud

While risk perception and familiarity provide context for how internal auditors view AI-enabled fraud, they do not fully explain where concerns concentrate in practice. Because AI is highly versatile and can be exploited by threat actors to carry out a wide range of fraudulent activities, a Chief Information Security Officer within a large audit and risk management technology organization identified the most salient AI-enabled fraud risks in this emerging area. Survey respondents could select all applicable risks from the resulting list. AI-powered phishing attempts were the most frequently cited concern (88%), followed by the use of fabricated invoices or financial documents (65%), and automated social engineering (58%).

FIGURE 2

Top concerns of AI-enabled fraud



Q15: Which types of AI-enabled fraud do you perceive as the most concerning for your organization? (Choose all that apply) n=373.

Beyond these leading concerns, findings also reveal differences in how organizations perceive less visible but quickly growing risks. For example, synthetic identity fraud, which creates fake identities by blending real and bogus information, was rated as the lowest area of concern among respondents (27%), despite external research identifying it as the fastest-growing financial crime in the U.S., with estimated total losses exceeding $5 billion.[9] This suggests that some AI-enabled fraud risks remain under-recognized, specifically those more difficult to detect. Figures 3 and 4 illustrate how individuals can easily generate financial documents using widely accessible AI platforms, such as OpenAI's ChatGPT.

Although these examples appear plausible at first glance, they also exhibit telltale signs of AI-generated content, such as mismatched or overlapping formatting, small math errors, or inconsistent logo/barcode placement. Recognizing these indicators may help risk professionals identify discrepancies earlier and strengthen controls designed to protect their organizations from financial loss.

FIGURE 3

AI-generated receipt

Cafe de Flor

12 Rue des Fleurs, Paris
Tel: +33 1 23 45 67 89

Date: 2025-11-04 18:22 Cashier: Marie

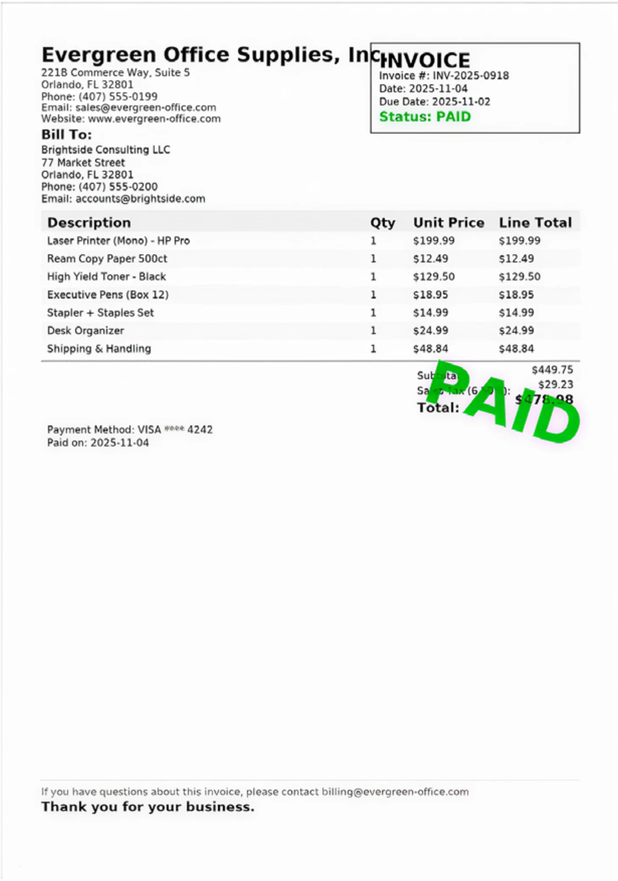
Almond Croissant	€3.45
Butter Croissant	€2.95
Blueberry Muffin	€3.50
Caffe Latte	€4.20
Espresso	€2.10
Orange Juice	€9.56
Subtotal	€25.76
VAT (incl.)	€2.58
Total	**€25.76**

Thank you for visiting Cafe de Flor

A ChatGPT-generated receipt using the following prompt: "Create a receipt that looks like it was photocopied from a café in Paris. Make the total 25.76 and ensure the transaction date is on 11-4-2025."

FIGURE 4

AI-generated invoice



Evergreen Office Supplies, Inc.
2218 Commerce Way, Suite 5
Orlando, FL 32801
Phone: (407) 555-0199
Email: sales@evergreen-office.com
Website: www.evergreen-office.com

INVOICE
Invoice #: INV-2025-0918
Date: 2025-11-04
Due Date: 2025-11-02
Status: PAID

Bill To:
Brightside Consulting LLC
77 Market Street
Orlando, FL 32801
Phone: (407) 555-0200
Email: accounts@brightside.com

Description	Qty	Unit Price	Line Total
Laser Printer (Mono) - HP Pro	1	$199.99	$199.99
Ream Copy Paper 500ct	1	$12.49	$12.49
High Yield Toner - Black	1	$129.50	$129.50
Executive Pens (Box 12)	1	$18.95	$18.95
Stapler + Staples Set	1	$14.99	$14.99
Desk Organizer	1	$24.99	$24.99
Shipping & Handling	1	$48.84	$48.84

$449.75
$29.23
Total: $478.98

PAID

Payment Method: VISA **** 4242
Paid on: 2025-11-04

If you have questions about this invoice, please contact billing@evergreen-office.com
Thank you for your business.

A ChatGPT-generated invoice using the following prompt: "Create a paid invoice for a company that sells office supplies. Make the total $478.98."

Frequency of AI-enabled fraud

More than one-third of senior internal audit leaders (34%) reported uncertainty about whether their organizations were targets of such fraud attempts. While nearly half (48%) said their organizations had not been targeted, and another 18% reported being aware of one or more instances, the level of uncertainty highlights the awareness gap identified earlier, potentially creating material implications for organizations.

To better understand how AI-enabled fraud unfolds in practice respondents shared firsthand accounts. Figure 5 provides a selected sample of the accounts.

FIGURE 5

Accounts of AI-enabled fraud and the challenges of detection

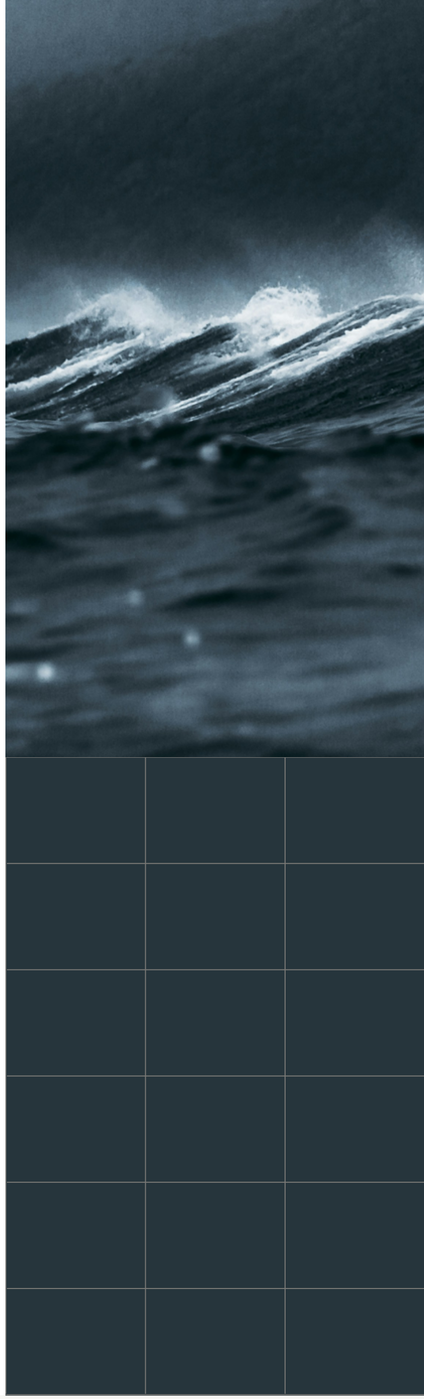
"Prospective customers submit fraudulent applications using AI-generated ID's or 'selfies' and other information to validate legitimacy."

"Our call center has received multiple 'deep-fake' calls, and we have received documents requesting withdrawals that appear to have been created using AI..."

"[We have experienced] AI-assisted phishing attempts with fraudulent web-based form submissions... IT has since revised our web-based form to include a check for human entry, reducing fraudulent submissions."

"AI was used to attempt to have fictitious vendors set up and payments remitted."

Q18: Please describe the nature of the incident(s), including how AI was utilized and the challenges it posed for detection. Kindly refrain from including any sensitive or personally identifiable information. (Optional) n=23.



Understanding how AI-enabled fraud manifests in real-world examples provides important context, situating this emerging risk. However, the true impact of internal audit emerges through how it evaluates and responds to the risk, offering assurance and strategic guidance. Figure 6 shows the various ways in which internal audit functions currently engage. The most frequently cited activities include:

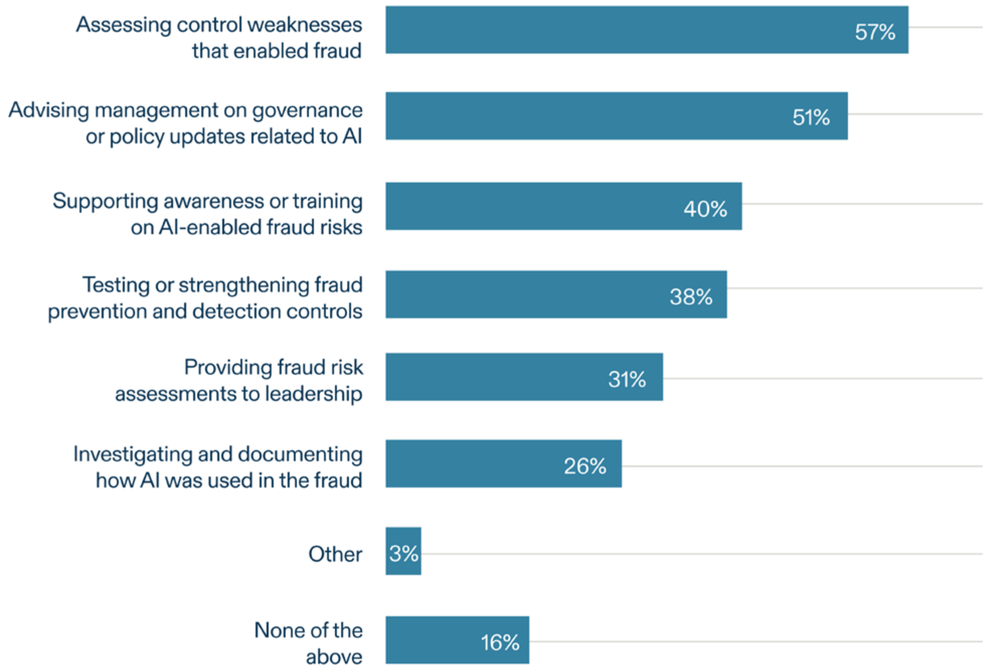
- Assessing control weaknesses (57%)
- Providing strategic advising on governance and policy updates (51%)
- Supporting awareness training (40%)

These insights indicate internal audit's current role remains largely conventional, focused on evaluating control effectiveness and providing recommendations to strengthen controls and inform organizational decision-making.

Internal audit contributes to deterrence and response primarily through assurance and insight, alongside management and other functions that hold operational responsibility. Their unique position within the organization provides a valuable advantage from which to assess both organizational preparedness and resilience to this emerging risk. As AI capabilities become more embedded across organizational processes, internal audit faces an opportunity to expand its role further. This includes greater engagement with leadership in developing fraud risk assessments, ensuring decision-makers are informed about the potential misuse of AI, and strengthening assurance by becoming more involved in investigating and documenting AI-related fraud incidents. By applying specialized knowledge of AI misuse, internal audit can also advise organizations on designing and/or reinforcing more robust and risk-sensitive controls.

FIGURE 6

Internal audit response to AI-enabled fraud



Q17: In what ways has internal audit been involved in responding to those instances of fraud? (Choose all that apply.) [Shown if AI-enabled fraud has been experienced per Q16] n=68.

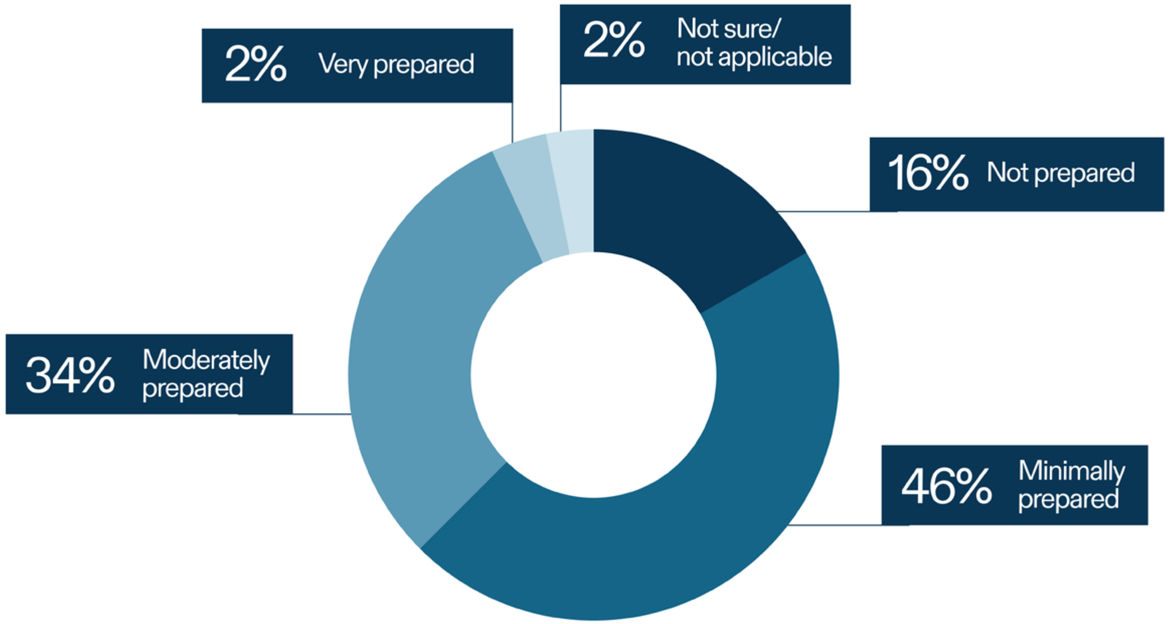
Current preparedness and barriers

It's critical to assess whether internal audit teams remain prepared to engage in AI-enabled fraud risk management. Findings from the study reflect an opportunity to ensure functions are well-prepared to address this burgeoning risk. As shown in Figure 7, more than six in 10 of those surveyed (62%) said their internal audit function is either unprepared or minimally prepared to detect AI-enabled fraud, with only 36% saying their function is moderately or very prepared.

These numbers provide a high-level view of how internal auditors perceive their ability to respond if AI-enabled fraud were to occur. Examining the underlying barriers shaping these perceptions reveals additional structural challenges. More than half of respondents cited a lack of appropriate technology or tools (57%) and insufficient staff with relevant skills or expertise (55%) as the most significant obstacles. Resource constraints further compound these challenges, with nearly half pointing to limited financial budgets (46%), competing organizational priorities (43%), and insufficient time (43%) to dedicate to AI-specific risk management efforts.

FIGURE 7

Preparedness of internal audit team in detecting AI-enabled fraud



Q20: How prepared is your internal audit team to detect AI-enabled fraud? n=372.

Current and future use of AI in internal audit activities

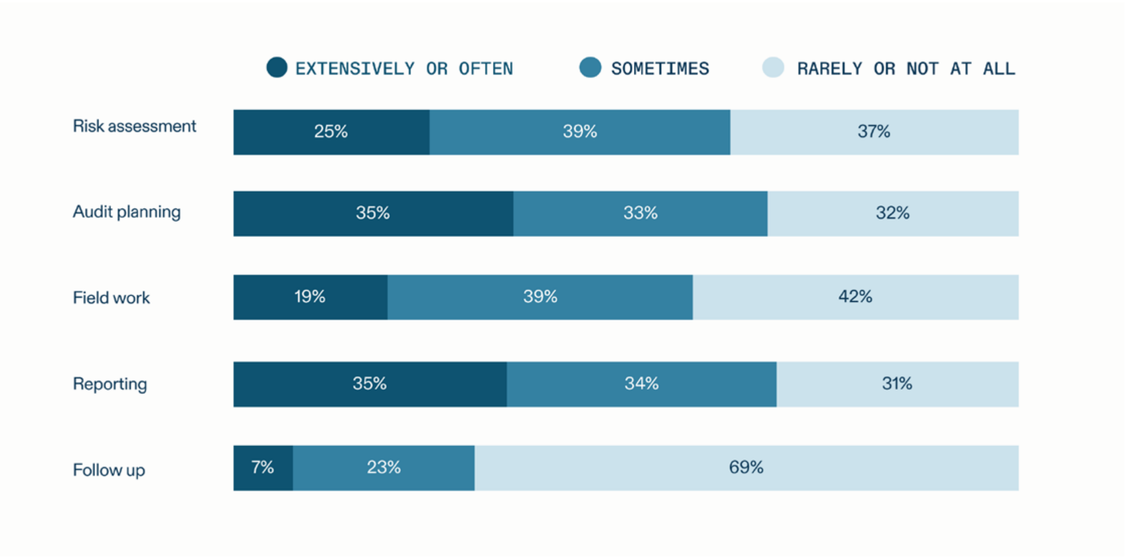
Figure 8 highlights how internal audit currently uses AI across a range of tasks, supporting both efficiency and analytical depth. The growing use of AI within internal audit suggests a baseline level of familiarity with how these technologies operate in practice.

Auditors can strategically leverage that familiarity as they engage in advisory activities related to AI governance, policy development, control evaluation, and risk assessment and mitigation. Effective auditing requires hands-on experience. By using AI, auditors build the technical understanding needed to distinguish legitimate activity from AI-enabled fraud.

A majority (83%) of respondents stated their internal audit function plans to increase the use of AI over the next year. This underscores the need for internal auditors to stay well-informed about AI's potential misuse, both within internal audit and across the organization. Developing a more nuanced understanding of this rapidly advancing technology's capabilities and limitations, along with the skills needed to engage with it, can help internal auditors recognize the risks associated with improper or malicious use. This future-focused knowledge is critical for strengthening internal audit's ability to assess controls, advise management, and anticipate emerging AI-enabled fraud risks.

FIGURE 8

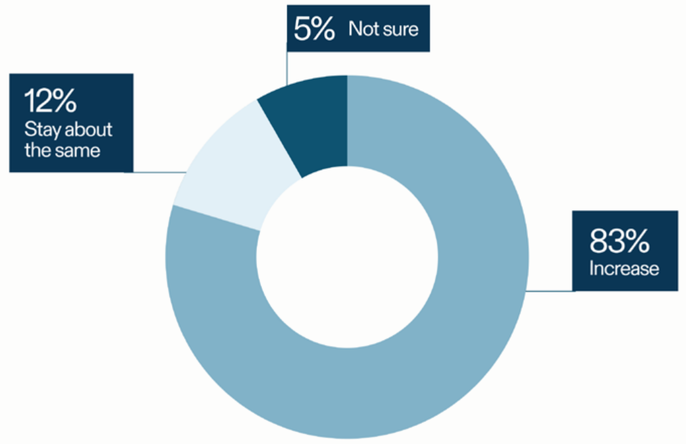
Current use of AI to support internal audit activities



Q32: Please indicate to what extent your internal audit function is using AI to support the following internal audit activities. n=373. Note: row totals may not equal 100% due to rounding.

FIGURE 9

Future AI usage by internal audit



Q31: Over the next year, do you plan to increase or decrease use of AI within your internal audit function? n=373.

Priority actions for AI-enabled fraud readiness

A key focus was to gather insights from practitioners on the single most important action internal auditors can prioritize to prepare for this risk. Comments centered on three key themes.

1. Skill building

By far, the most prevalent theme emphasized the need for continuous and regularly updated training focused on building and testing skills. Respondents consistently highlighted that training must be adaptive, evolving alongside AI's rapidly expanding capabilities and associated fraud risks.

Skill development is an ongoing process designed to keep internal auditors up to date on emerging AI-enabled fraud techniques. This might involve practical exercises in which internal auditors test their skills in a controlled environment Internal organizational initiatives can deliver skill-building efforts, or external firms or consultants with specialized expertise can supplement them. The objective in both cases is to ensure that internal auditors and the broader organization develop the knowledge and practical competencies needed to identify, assess, and deter AI-enabled fraud.

Importantly, respondents noted that skill-building can scale based on organizational maturity and risk exposure. This ranges from foundational awareness training for broad audiences to more advanced upskilling, specialized training, or formal certification for auditors with deeper responsibilities related to AI-enabled fraud detection and deterrence.

2. Alignment on AI use

A substantial number of responses emphasized the importance of organizational alignment on AI use across the enterprise. Respondents highlighted the need for greater visibility into where and how AI is embedded in business processes, often citing the value of AI inventories and structured inquiries across business units. This broader understanding enables internal audit to incorporate organization-wide AI considerations into audit planning, risk assessments, and audit procedures.

Internal audit leaders also made clear that efforts to deter and address AI-enabled fraud cannot remain siloed. Instead, they require governance and coordination that can keep pace with this rapidly evolving risk environment. Alignment across the organization helps ensure that AI-related risks, including fraud, are consistently identified, assessed, and managed, rather than addressed in a fragmented or reactive manner.

3. Collaboration

Respondents consistently described effective preparation as a shared responsibility that requires close coordination with technology, cybersecurity, and risk management teams. Respondents also noted the value of engaging business units that may already have greater experience with AI and related technologies, particularly in organizations where AI use and awareness are still emerging.

Leaders also framed collaboration not only as knowledge-sharing, but also as a means of enabling more effective detection and mitigation efforts. By working across functions, internal audit can better understand how AI is deployed, leverage existing technical expertise, and ensure that appropriate safeguards are in place. Overall, respondents underscored the importance of collaboration and adequate resourcing that extends beyond training and organizational alignment.

Conclusion

While this report provides timely and relevant insights into the risk of AI-enabled fraud and the current understanding of AI across the risk landscape, its scope is limited to North America. It primarily reflects the perspectives of senior internal audit leadership. It is not intended to offer an exhaustive assessment of all the ways AI may be used, for good or for harm. Rather, it serves as a foundational reference point for audit functions globally as they assess their own organizational needs, maturity, and preparedness. While internal audit standards and guidance are largely consistent globally, AI regulation and related legal requirements may vary significantly by jurisdiction, further influencing how organizations understand and manage risks.

Respondents consistently emphasized that effective response to AI-enabled fraud requires both collaboration and targeted upskilling. A critical first step is harnessing existing AI knowledge across the organization to identify gaps, anticipate how bad actors can exploit AI, and determine the need for targeted training. Regardless of audit function size, industry, or resource constraints, internal auditors at all levels can take meaningful action today to strengthen their understanding of the evolving risks associated with AI misuse. AI is uniquely positioned as a dual-use capability, one that simultaneously accelerates fraud risk and enhances the ability to detect and prevent it. How internal audit engages with this reality will shape its relevance and impact within the organization going forward.

References

1. Eric Lamarre, Alex Singla, Alexander Sukharevsky, and Rodney Zemmell, A Generative AI Reset: Rewiring to Turn Potential Into Value in 2024 (New York: McKinsey & Company, March 2024), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/a-generative-ai-reset-rewiring-to-turn-potential-into-value-in-2024.
2. LexisNexis Risk Solutions. 2022. Global State of Fraud and Identity Report. LexisNexis Risk Solutions. https://risk.lexisnexis.com/insights-resources/research/global-state-of-fraud-and-identity.
3. Blake Hall, "How AI-Driven Fraud Challenges the Global Economy – and Ways to Combat It," World Economic Forum, January 16, 2025, https://www.weforum.org/stories/2025/01/how-ai-driven-fraud-challenges-the-global-economy-and-ways-to-combat-it/.
4. The Institute of Internal Auditors, Global Internal Audit Standards (Lake Mary, FL: The Institute of Internal Auditors, January 9, 2024), https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/free-documents/complete-global-internal-audit-standards/.
5. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0) (Gaithersburg, MD: NIST, January 26, 2023), https://doi.org/10.6028/NIST.AI.100-1.
6. Stefan Feuerriegel, Jochen Hartmann, Christian Janiesch, and Patrick Zschech, "Generative AI," Business & Information Systems Engineering 66, no. 1 (2024): 111–126, https://doi.org/10.1007/s12599-023-00834-7.
7. Ajay Bandi, Bhavani Kongari, Roshini Naguru, Sahitya Pasnoor, and Sri Vidya Vilipala, "The Rise of Agentic AI: A Review of Definitions, Frameworks, Architectures, Applications, Evaluation Metrics, and Challenges," Future Internet 17, no. 9 (2025): 404, https://doi.org/10.3390/fi17090404.
8. Chandra Khatri, Anu Venkatesh, Behnam Hedayatnia, Ashwin Ram, Raefer Gabriel, and Rohit Prasad, "Alexa Prize: State of the Art in Conversational AI," AI Magazine 39, no. 3 (2018): 40–55, https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/2810.
9. Internal Audit Foundation, Risk in Focus 2026: Global Summary. (Lake Mary, FL: Internal Audit Foundation, 2025), https://www.theiia.org/globalassets/site/foundation/latest-research-and-products/risk-in-focus/2026/2026-global-report-en-riskinfocus.pdf.
10. Internal Audit Foundation, 2025 North American Pulse of Internal Audit (Lake Mary, FL: Internal Audit Foundation, 2025, Accessed January 6, 2026), https://www.theiia.org/globalassets/site/resources/research-and-reports/pulse-of-internal-audit/2025-iia-pulse-report.pdf.

Appendix

Survey demographics

Primary industry classification	%	n
Finance and insurance	27%	99
Educational services	14%	51
Manufacturing	13%	47
Public administration	10%	37
Health care and social assistance	8%	30
Other services (except public administration)	5%	18
Utilities	4%	16
Transportation and warehousing	4%	16
Professional, scientific, and technical services	3%	13
Retail trade	3%	12
Information	2%	9
Mining, quarrying, and oil and gas extraction	2%	7
Agriculture, forestry, fishing, and hunting	1%	4
Accommodation and food services	1%	3
Arts, entertainment, and recreation	1%	3
Management of companies and enterprises	1%	3
Construction	1%	2
Administrative and support, waste management, and remediation services	0%	1
Real estate, rental, and leasing	0%	1
Wholesale trade	0%	1
NET	100%	373

Organization type	%	n
Financial services	26.54%	99
Publicly traded	27.08%	101
Privately held	7.77%	29
Nonprofit	9.12%	34
Public sector	27.61%	103
NET	98.12%	366

Organization size	%	n
500 or fewer	15.32%	57
501 to 1,500	16.94%	63
1,501 to 5,000	25.27%	94
5,001 to 10,000	14.52%	54
10,001 to 50,000	23.92%	89
More than 50,000	4.03%	15
NET	100%	372

Internal audit function size	%	n
1 to 3	17.16%	64
4 to 9	35.39%	132
10 to 24	34.32%	128
25 to 49	6.70%	25
50+	6.43%	24
NET	100%	373

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 260,000 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 the preeminent global resource, in strategic partnership with The IIA, dedicated to elevating and empowering the internal audit profession by developing cutting-edge research and programs. For 50 years, the Foundation has helped current and future internal auditors stay relevant by building and enhancing their skills and knowledge, ensuring organizations are equipped to create, protect, and sustain long-term value. For more information, visit theiia.org/Foundation.

IIA Internal Audit Foundation

2025–26 Board of Trustees

President

Glenn Ho, CIA, CRMA

Senior Vice President – Strategy

Shirley Livhuwani Machaba, CCSA, CRMA

Vice President – Finance and Development

Michael A. Smith, CIA

Vice President – Content

Nora Zeid Kelani, CIA, CRMA

Trustees

Mohammed Al Qahtani, CIA

Jose Gabriel Calderon, CIA, CRMA

Reyes Fuentes Ortea, CIA, CCSA, CRMA

Susan Haseley, CIA

Dawn Jones, CIA, CRMA

Anthony J. Pugliese, CIA

Nicholas C. Saracco, CIA

Bhaskar Subramanian

Staff Liaison

Laura LeBlanc, Senior Director, Internal Audit Foundation

2025–26 Committee of Research and Education Advisors (CREA)

Chair

Nora Zeid Kelani, CIA, CRMA

Members

Tonya Arnold-Tornquist, CIA, CRMA

Christopher Calvin, Ph.D., CIA

Joseph Ian Canlas, CIA, CRMA

Andrew Dahle, CIA, CRMA

Andre Domingos

Christina Duquette, CRMA

Marc Eulerich, Ph.D., CIA

Dagmar Flores, CIA, CCSA, CRMA

Ivony Kudzayi Katsande-Zezekwa, D.B.L., CIA, CRMA

Ayaka Mitsunari, CIA

Ahmed Shawky Mohammed, D.B.A., CIA

Grace Mubako, Ph.D., CIA

Emmanuel Pascal, CIA, CRMA

Brad Schafer, Ph.D., CIA

Brian Tremblay, CIA

Koji Watanabe

Stacy Wright, CIA

Staff Liaison

Nicole Narkiewicz, Ph.D., IAP, Director, Internal Audit Foundation

Project contributors

Dillon Caldwell, Ph.D.

Marc Eulerich, Ph.D., CIA

Nicole Narkiewicz, Ph.D., IAP

Emmanuel Pascal, CIA, CRMA

Brian Tremblay, CIA

About AuditBoard

AuditBoard's mission is to be the category-defining global platform for connected risk, elevating our customers through innovation. More than 50% of the Fortune 500 trust AuditBoard to transform their audit, risk, and compliance management. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the sixth year in a row as one of the fastest-growing technology companies in North America by Deloitte.