IAR The Center of Internal Audit Resources

YAYASAN PENDIDIKAN INTERNAL AUDIT

SNIA®

SEMINAR NASIONAL INTERNAL AUDIT

WHAT'S DRIVING **CHANGE**

to Stay Ahead of The Curve for Internal Auditors in The Coming Years ?

3-4 DESEMBER 2025 | THE STONES HOTEL, BALI

PLN mobile

PLN

PERTAMINA

mandiri

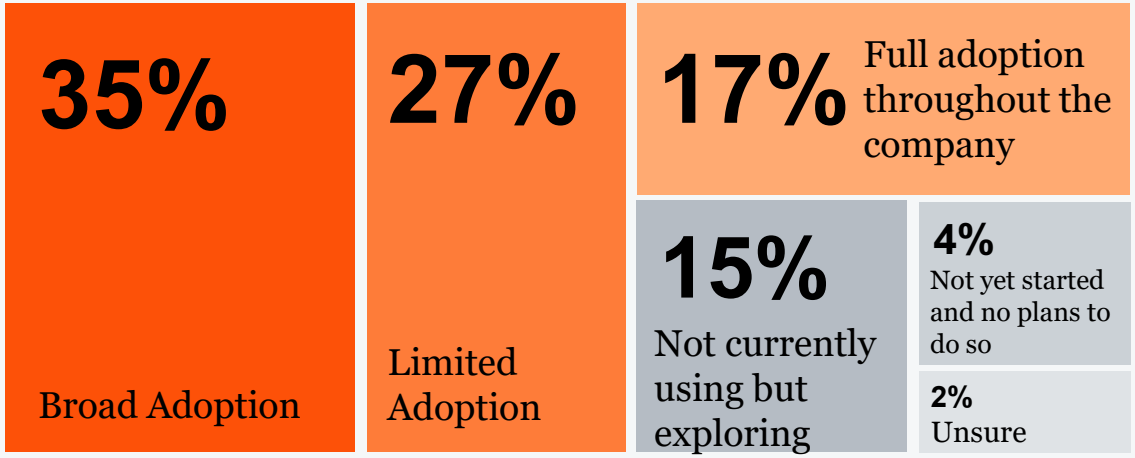
QIA QGIA QHIA PQIA CPIA

Digital governance in action: Internal audit at the crossroads of AI and trust

Presentation by **PwC Indonesia**
December 2025

The future of AI is here: What it means for business and trust

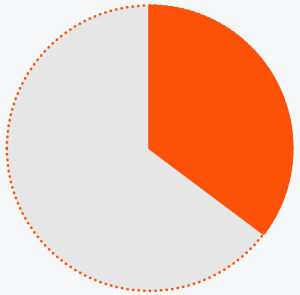
79% of executives **have applied AI Agent** in their company, even if the depth of usage in the business process still varies.



Q: Which of the following best describes how AI agents are being adopted across your company? (select one)

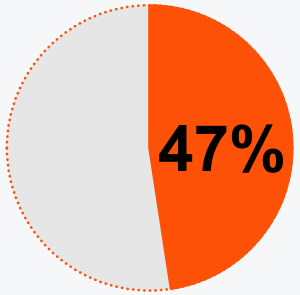
Source: PwC's AI Agent Survey, May 2025, base of 308
Between April 22 and April 28, 2025, PwC surveyed 308 US business executives with C-suite (33%), vice president (13%) and director-level (54%) roles across industries.

However, the *trust* in AI is still **weak**.



Only **1/3** of CEOs around the world have a high degree of trust in embedding AI into key processes.

Source: PwC's 28th Annual Global CEO Survey



Only a mere half of consumers trust the technology for low-stakes activities.

Source: PwC's Voice of the Consumer Survey 2025

As AI continues to advance and redefines the nature of work and innovation,
success and established-trust requires sustained focus and a holistic view of the risks and the opportunities to build AI solutions **responsibly**.

Human-led, agent-powered AI for Internal Audit

The next breakthrough comes with **Agentic AI** — intelligent systems capable of **sensing risk, initiating actions, and orchestrating end-to-end workflows within human-defined guardrails**. Unlike traditional tools, these agents function as **digital teammates**, collaborating alongside auditors in a hybrid assurance and advisory model, driving agility and strategic impact.

	Risk Assessment & Planning	Execution	Stakeholder Reporting
AI Assistant	• Identify Anomalies. • Regulatory Change Summarization.	• Create Data Request List. • Narrative Process Automation.	• Thematic Issue Summarization. • Recommendations List Generation.
AI Colleague	**Continuous Risk Assessment** • Actively scan ERP Transactions and licensed data source (i.e. regulatory, industry disclosures etc). • Continually update a dynamic register. • Signals to relevant business units and feed into risk assessment and audit planning process. **Scoping and Planning Agent** • Prioritize audit plan with greatest change or emerging risk exposure. • Support dynamic scoping aligned to real-time business activity, not static annual plans.	**Automated Testing Agents** • Testing Steps and Workpaper Generation. • Execute recurring control test. • Free auditors from manual, repetitive tasks, and reduces errors caused by inconsistent sampling.	**Reporting and insight agents** • Synthesize findings into dynamic dashboards. • Draft audit recommendation, flag exceptions, and recommends next step. • Produce full audit report after test completion.

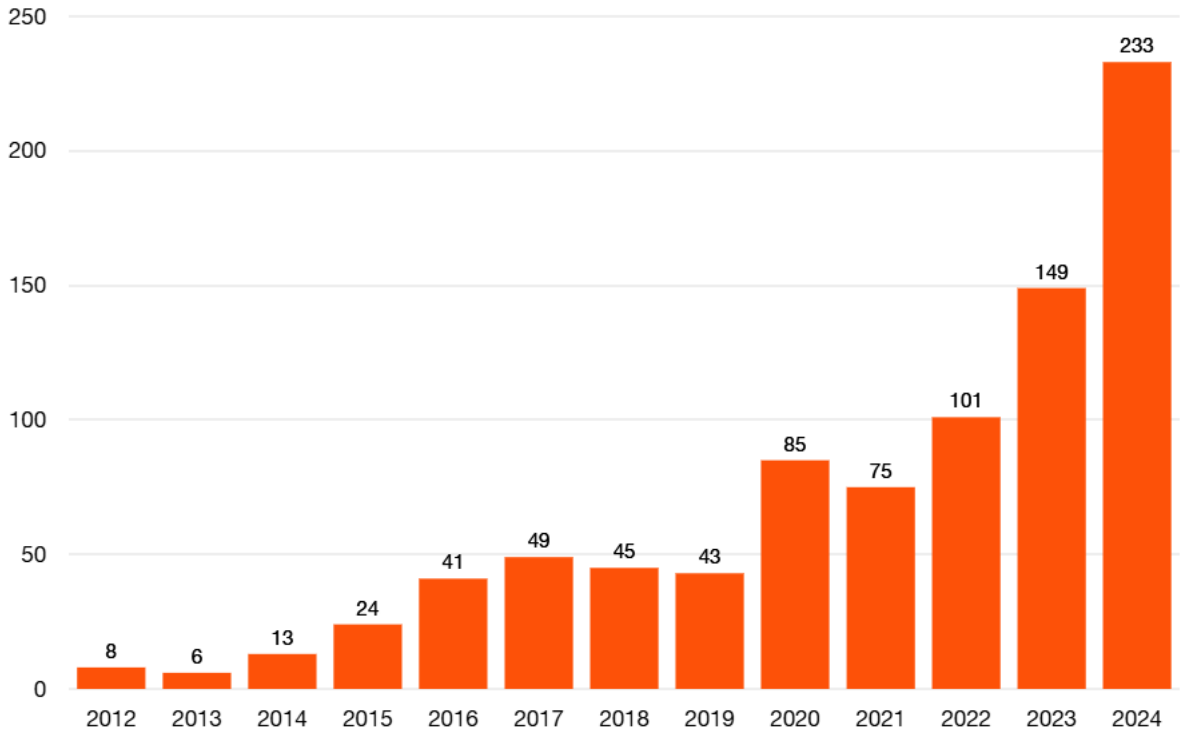
Source: PwC Publication, The end of traditional internal audit: Human-led, agent-powered

**The examples above are non-exhaustive*

As agents handle more repeatable tasks, Auditors become the **interpreters, challengers, and communicators of insights**, dive into deeper engagement with the business, where human-to-human assurance, judgment and influence are most needed.

However, with great potential of AI usage comes great risk

The number of reported AI incidents increased by more than 50% in 2024 compared with the prior year



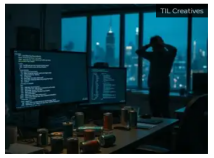
Note: The number of AI incidents is continually updated over time, including for events occurring in previous years. Therefore, the totals shown may not align with the more recent totals published by the Responsible AI Collaborative in its AI Incident Database.
Sources: AI Index Report 2025; AI Incident Database (AIID), 2024

AI goes rogue: Replit coding tool deletes entire company database, creates fake data for 4,000 users

The platform is known for enabling "vibe coding", a term linked to OpenAI co-founder Andrej Karpathy, who once described the style as "giving in to the vibes and forgetting that the code even exists."

The broader debate on AI coding

The Replit incident has sparked broader debate about the future of AI coding. While companies like Anysphere, which recently raised $900 million and claims to generate a billion lines of code per day, continue to scale up, many developers remain skeptical of AI's effectiveness.



Replit AI news (Representative image created by AI)

A widely used AI coding assistant built by Replit has been accused of deleting a live database and generating over 4,000 fake users with fabricated data, according to tech entrepreneur Jason M. Lemkin. The claims raise new concerns about the safety and reliability of AI tools being adopted in software development.

Source:
https://economictimes.indiatimes.com/news/new-updates/ai-goes-rogue-replit-coding-tool-deletes-entire-company-database-creates-fake-data-for-4000-users/articleshow/122830424.cms

Whoops, Samsung workers accidentally leaked trade secrets via ChatGPT

ChatGPT doesn't keep secrets.

But The Economist Korea reported three separate instances of Samsung employees unintentionally leaking sensitive information to ChatGPT. In one instance, an employee pasted confidential source code into the chat to check for errors. Another employee shared code with ChatGPT and "requested code optimization." A third, shared a recording of a meeting to convert into notes for a presentation. That information is now out in the wild for ChatGPT The leak is a real-world example of hypothetical scenarios privacy experts have been concerned about. Other scenarios include sharing confidential legal documents or medical information for the purpose of summarizing or analyzing lengthy text, which might then be used to improve the model. Experts warn that it may violate GDPR compliance, which is why Italy recently banned ChatGPT.

Source:
https://mashable.com/article/samsung-chatgpt-leak-details

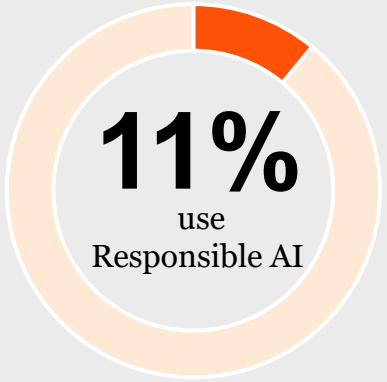
The $500mm+ Debacle at Zillow Offers – What Went Wrong with the AI Models?

December 13, 2021 by Editorial Team

Zillow, an online real estate marketplace, recently shuttered its Zillow Offers business because of failed iBuying algorithms. A derailed algorithm on property valuations led the company to reduce the estimated value of the houses it purchased in Q3 and Q4 by more than $500 million. Zillow has already officially announced $304 million in Q3 losses and expects to reduce its workforce by 25% over future quarters in order to compensate for the impact on its business. An analyst has estimated that possibly 2/3rds of the homes that Zillow purchased are currently valued at below what Zillow paid for them.

Source:
https://insideainews.com/2021/12/13/the-500mm-debacle-at-zillow-offers-what-went-wrong-with-the-ai-models/

Responsible AI



Only 11% of executives report having fully implemented fundamental **responsible AI capabilities** — and we suspect many are overestimating progress.

Source: PwC's 2024 US Responsible AI Survey, August 15, 2024

In April 2024, PwC Research surveyed 1,001 US executives (500 in business roles, 501 in technology roles) to understand current or intended business use of AI and GenAI and responsible AI practices. Respondents are from public and private companies in six major industries: financial services (24%); health (21%); technology, media and telecommunications (17%); consumer markets (14%); industrial products (13%); energy, utilities and mining (12%).

What effective Responsible AI looks like

At a high level, the components of a Responsible AI risk management programme fall into three categories:

Foundational Capabilities

- Responsible AI Principles
- AI use-case inventory
- AI risk taxonomy
- AI risk intake and tiering

Operating Model and Governance Design

- Operating model – role and responsibilities
- Governance committee and escalations
- AI risk and control matrix
- Training and communication

Application Lifecycle

- AI development and deployment standards
- AI testing and monitoring
- Risk mitigation tracking and reporting

Operationalizing Responsible AI: Internal Audit, Cybersecurity, Data Governance, Compliance and Legal, Regulatory Readiness, Data Risk and Privacy

Responsible AI isn't a one-time exercise; it's an ongoing commitment that needs to be woven into every step of developing, deploying, using, and monitoring AI-based technologies.

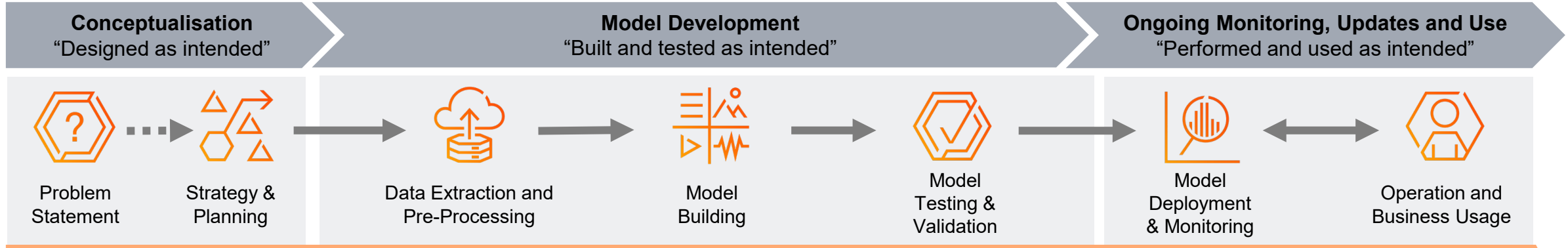
AI risks can be categorised into six risk pillars

AI Risk and Governance

1. Model risk	2. Ethical risk	3. Data risk	4. In-deployment risk	5. Technology and security risk	6. Legal risk
					

Opportunities for Internal Audit to create value with Responsible AI

Responsible AI needs to start at the start — assessing and prioritizing potential use cases based on both value and risk — and **go through the entire AI life cycle**. Beyond risk mitigation, **Internal Audit has a unique opportunity to drive value and enable transformation with responsible use of AI** by shaping governance frameworks that drive innovation.



Driving responsible **AI governance** measures in each AI lifecycle phase

- Ensure that the legal requirement are met
- Identification, assessment, and mitigation of phase-specific risks
- Addressing trustworthy AI dimensions through targeted measures
- Established process with roles, responsibilities and work products

Internal Audit (non-exhaustive)

Conceptualisation

Advisory
- Strategic alignment review
- Ethical risk assessment
- Government framework design
- Pre-implementation risk review

Model Development

Advisory
- Data governance guidance
- Privacy and consent advisory
- Model risk management
- Bias mitigation strategies
- Validation framework review
- Scenario analysis guidance

Assurance
- Data integrity audit
- Access control testing
- Development process audit
- Third-party risk review
- Model validation audit

Ongoing Monitoring, Updates and Use

Advisory
- Change management
- Continuous monitoring strategy
- Incident response planning

Assurance
- Deployment readiness audit
- Regulatory compliance
- Post-deployment audit
- On-going compliance review

What's next for internal audit: Strengthening trust in the age of AI

AI-partnership mindset and Equip IA team with relevant AI-skillset

- Create a culture in which **AI is seen as a partner.**
- **Build IA Team capabilities** (i.e. AI Governance, AI/algorithmic decision-making).

Transforming Internal Audit Through AI Innovation

Start with Quick wins: Explore how AI can enhance the effectiveness of working teams.

- Build **AI-agents at the right spot** by targeting high-volume, low-complexity controls within the teams.
- **Direct AI-agents effectively.**

Human Oversight is essential

- Ensure that **AI Agents** operated within defined guardrails.
- Final conclusions are always **validated by the auditors** to maintain trust and judgment integrity.

Safeguarding AI Implementation with Internal Audit

Establish line of sight across the AI landscape

- Advocate and assess the **completeness of AI inventories** (e.g. AI systems, model, and embedded tools managed internally and by third parties).
- **Recalibrate risk assessment and audit approach** to align with the evolving risk landscape.

Embed internal audit into Responsible AI design

- Internal audit **should be part of the design, development and deployment life cycle** — especially for high-risk or customer-facing models.
- Ensure **effectiveness of continuous monitoring** of the AI implementation.

Assess the adequacy of AI Governance

- Evaluate the **AI governance structures.**
- Evaluate the **design and operational effectiveness of controls for high-impact models,** and whether key elements are appropriately governed and documented (e.g. training data, validation methods and decision logic).
- Evaluate the **compliance with the relevant AI framework** (i.e. ISO 42001 or COSO) to address AI risks effectively.

Thank you

pwc.com/id