GRC CAREERS · AI GOVERNANCE GUIDE

10 Questions Every Chief Audit Executive Should Ask About AI Risk and Governance

Boards and regulators increasingly expect Chief Audit Executives to provide assurance that AI is governed responsibly. Here are ten questions every CAE should be asking, and why each one matters.

Artificial intelligence is transforming how organizations operate, but it is also introducing new risks that Internal Audit must understand. Boards, regulators, and executive leadership increasingly expect Chief Audit Executives (CAEs) to provide assurance that AI systems are governed responsibly.

Below are ten questions every CAE should be asking, along with why each question matters.

1. Do we know what AI our organization is using?

One of the biggest risks is not the AI you know about. It is the AI you do not.

Many organizations have employees experimenting with AI tools without formal approval. Creating and maintaining an inventory of AI systems is the first step toward effective governance.

Why it matters: You cannot audit what you cannot identify.

2. Who owns each AI system?

Every AI application should have a clearly identified business owner responsible for oversight, performance, and compliance. Ownership should include accountability for monitoring, documentation, risk management, and ongoing governance.

Why it matters: Without ownership, accountability quickly disappears.

3. Has every AI solution been risk assessed?

Not every AI system presents the same level of risk. Organizations should evaluate AI based on factors such as:

- Business impact
- Data sensitivity

- Regulatory exposure
- Customer impact
- Financial consequences
- Reputational risk

High-risk systems should receive greater oversight and more frequent review.

Why it matters: Risk-based auditing helps focus resources where they are needed most.

4. What data is being used and shared?

AI depends on data. Internal Audit should understand:

- What information is being entered into AI tools
- Whether confidential data is protected
- How personal information is handled
- Whether retention policies are followed
- Whether third-party vendors receive organizational data

Why it matters: Poor data governance creates legal, security, and privacy risks.

5. How are AI outputs validated?

Generative AI can produce incorrect or misleading information with great confidence. Organizations should establish procedures for reviewing AI-generated content before it influences important decisions. Questions include:

- Who reviews AI outputs?
- Are human approvals required?
- How are errors identified?
- Are testing procedures documented?

Why it matters: Human oversight remains one of the strongest AI controls available.

6. Are employees using unauthorized AI tools?

Shadow AI is becoming a growing concern. Employees may use public AI platforms without realizing they are exposing confidential information. Audit should determine:

- Which AI tools are approved
- Whether monitoring exists
- Whether acceptable-use policies are enforced

- How unauthorized use is detected

Why it matters: Unauthorized AI creates security and compliance risks that often go unnoticed.

7. What documentation exists?

Strong governance depends on documentation. High-risk AI systems should include documentation covering:

- Business purpose
- Data sources
- Model limitations
- Testing procedures
- Validation results
- Responsible owners
- Monitoring plans

Why it matters: Good documentation supports transparency, repeatability, and regulatory readiness.

8. How is AI monitored over time?

AI systems change. Models may drift, vendors release updates, and business processes evolve. Internal Audit should ask:

- Are performance metrics tracked?
- Is model drift monitored?
- Are changes documented?
- Are periodic reviews scheduled?

Why it matters: AI governance is an ongoing process, not a one-time project.

9. How are third-party AI risks managed?

Many organizations rely on AI provided by software vendors. Internal Audit should evaluate:

- Vendor due diligence
- Contract protections
- Security controls
- Privacy practices

- Transparency regarding model development
- Incident response capabilities

Why it matters: Third-party AI can introduce significant organizational risk.

10. Are we ready for changing AI regulations?

The regulatory landscape continues to evolve rapidly. Chief Audit Executives should understand how the organization is preparing for emerging requirements, including:

- AI governance policies
- Industry standards
- Privacy regulations
- Documentation requirements
- Independent oversight
- Board reporting

Organizations that prepare today will be better positioned to adapt tomorrow.

Why it matters: Compliance is much easier when governance already exists.

Final thoughts

Artificial intelligence is reshaping the audit profession. The organizations that succeed will be those that establish strong governance before problems emerge.

By asking these ten questions, Chief Audit Executives can help strengthen oversight, build trust with leadership and the board, and position Internal Audit as a strategic partner in responsible AI adoption. Strong AI governance begins with asking the right questions.

Frequently asked questions

Does Internal Audit need AI experts?

No. Most audit teams do not need to build AI models. They do need enough knowledge to evaluate governance, controls, risk management, and compliance.

Should Internal Audit own AI governance?

Generally, no. Management owns AI governance. Internal Audit provides independent assurance that governance processes are designed and operating effectively.

What is Shadow AI?

Shadow AI refers to employees using AI tools without organizational approval or oversight. These tools may expose confidential information, create compliance issues, or introduce cybersecurity risks.

How often should AI systems be audited?

The audit frequency should reflect the level of risk. High-impact AI systems may require continuous monitoring or more frequent reviews, while lower-risk applications can often be assessed through periodic audits.

What skills should today's Chief Audit Executive develop?

Modern audit leaders benefit from understanding AI governance, enterprise risk management, cybersecurity, data governance, privacy, third-party risk, regulatory developments, and responsible AI principles.