Crowe

Internal auditor's AI safety checklist

Your role as an internal auditor matters.

Emerging technologies like artificial intelligence (AI) present an incredible opportunity in our field, but it's critical to understand the risks and rewards that come with them.

Use the following checklist to help get ahead of threats and safeguard data privacy when using AI tools that can make your day to day easier, more productive, and more fulfilling.

Are you using AI safely?

Following are five questions to explore.

1. Do you have a clear understanding of the AI systems being used in your organization?

A clear understanding of your AI systems can help empower you to:

- Make informed, strategic decisions
- Support responsible technology use and reduce risk
- Assess system performance, efficiency, and accuracy
- Meet compliance standards and regulations

☐	Yes! I have a strong and clear understanding of our AI systems.
☐	No, not yet – but I'll make sure to prioritize understanding our AI systems before moving forward.

2. Are the correct controls in place?

Internal auditors play a crucial role in helping organizations maintain well-designed, ethical, and effective filters that safeguard the integrity of:

- Data accuracy
- Legal and compliance standards
- Security measures
- Strategic decision-making

☐	Yes! The correct filters are in place, and I can move forward securely.
☐	No, not yet – but I'll make sure the correct filters are applied before I begin my audit.

3. Has access been authorized?

Securing the appropriate authorization helps mitigate risks, build trust, and promote successful AI applications. This step is crucial for internal auditors that need to uphold:

- Data privacy and security
- User trust
- Ethical standards and accountability
- Legal compliance

☐	Yes! Appropriate access has been granted to the right people.
☐	No, not yet – but I'll make sure proper access is granted before beginning the audit process.

4. Have data processing and collection policies been reviewed?

All data collection, storage, and processing policies need to be reviewed so that data is handled in compliance with existing privacy regulations. This review can help internal auditors with:

- Continual improvement
- Transparency and accountability
- Risk, consent, and vendor management
- Effective employee training and awareness

☐	Yes! Data processing and collection policies have been reviewed.
☐	No, not yet – but I'll make sure policies are reviewed before enacting the audit plan.

5. Have data quality and security been assessed?

AI is only as good as the data it has to work with. Evaluating data quality and security before beginning an internal audit is necessary for maintaining:

- Audit accuracy and reliability
- Resource efficiency
- Stakeholder confidence
- Risk mitigation

☐	Yes! Data quality and security have been assessed.
☐	No, not yet – but I'll make sure data quality and security are assessed before starting.

Did you answer yes to any or all of the 5 questions?

Great! Addressing these steps can help you perform your audit with confidence. Data is a critical asset for the organizations we serve. As internal auditors, we must maintain the integrity and safety of these assets and continue to provide strategic and valuable insights for the organizations we serve.

Did you answer no to any of these questions?

Don't worry. Crowe can provide the additional support you need as you continue navigating the crossroads of internal audit and AI.

Crowe

Check a successful audit off your list.

Reach out to Mike and let us be your guide.

Mike Varney
Partner, Consulting
+1 216 623 7553
mike.varney@crowe.com

Email Mike

CDUW2499-002B