

Driving trust in AI through governance and controls

Deloitte Trustworthy AI™ Solutions: **Audit and Assurance**

Audit and Assurance (A&A) artificial intelligence (AI) governance and controls advisory-related services include supporting clients by designing, assessing, challenging, and validating the current design and effectiveness of their AI governance frameworks and controls, either working directly with management (first and second line) or as part of the internal audit function (third line). We provide recommendations to enhance AI risk and control frameworks to help meet anticipated regulatory standards, are equipped to address the complexities of AI systems, and are designed to drive business value at both the program and use case levels. In addition, and aligned with professional standards, we provide independent attestations related to AI systems, controls, and governance against suitable criteria and legal and technical requirements, informed by ethical considerations.

As AI transforms business operations and scales within enterprises, organizations need to evolve governance, controls, oversight structures, and related processes to promote trust and transparency in the AI systems they deploy. These technologies can fundamentally change how work gets done and enable significant gains and they also introduce new and often less visible sources of risk.

While some AI systems operate on fixed, predefined rules, others infer patterns and make decisions based on inputs, model design, assumptions, and operating context. As a result, risks can emerge from multiple sources, including model design choices, shifting inputs, unintended bias, lack of transparency, and misalignment between model outputs and real-world expectations. Even subtle changes in inputs, usage context, or system interactions can lead to unexpected or inconsistent outcomes.

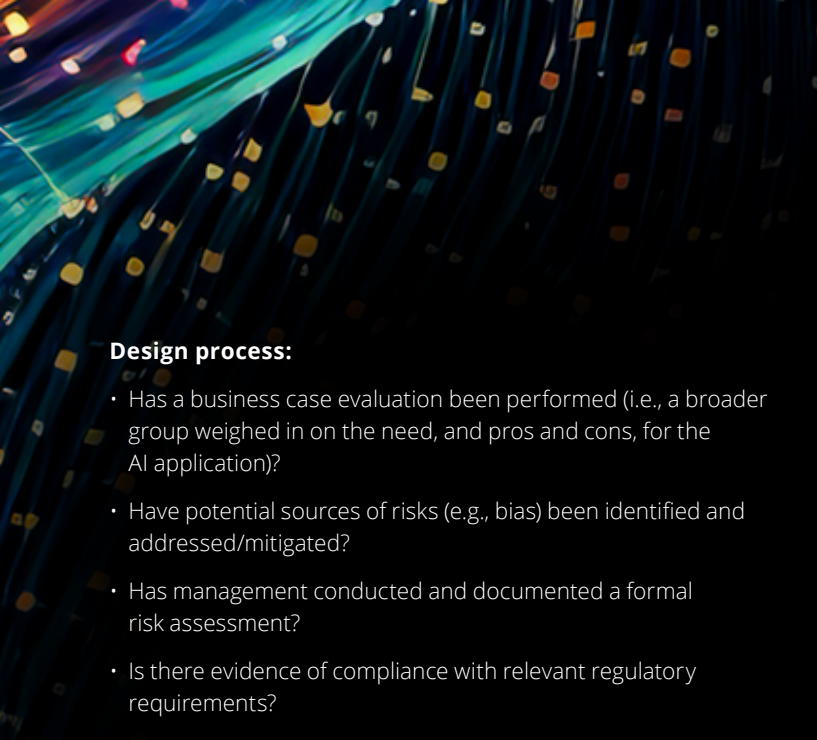
To manage and address these risks, organizations should implement extensive governance, controls, and monitoring practices across the full AI life cycle such that they can assess whether the models remain reliable and aligned with intended objectives as conditions evolve and course correct/remediate as needed.

Start with what you have

Organizations rely on governance and oversight structures for the effective design and operation of traditional technology applications, whether they are based on simple spreadsheets or sophisticated technology systems. In designing governance and oversight structures, organizations should consider the following:

Governance:

- Has management established and documented clear goals and objectives that articulate the purpose of deploying models and an AI program?
- Is there evidence of board-level oversight and approval of the AI strategy?
- Does the entity have a values or ethics statement applicable to the AI program?
- Are the roles and responsibilities for personnel involved with the governance, development, deployment, management and monitoring of AI programs defined?
- Does the governance program include appropriate preventative and detective controls that address risks including financial reporting and fraud risks?



Design process:

- Has a business case evaluation been performed (i.e., a broader group weighed in on the need, and pros and cons, for the AI application)?
- Have potential sources of risks (e.g., bias) been identified and addressed/mitigated?
- Has management conducted and documented a formal risk assessment?
- Is there evidence of compliance with relevant regulatory requirements?

Data:

- Is there a process for how data streams are selected and evaluated?
- Is there evidence of appropriate data security controls?
- Are there controls to ensure the completeness and accuracy of data inputs that affect financial reporting elements?
- Are datasets validated to ensure they are representative of the underlying populations and operational environment?

Development & Implementation:

- Is there evidence of appropriate segregation of duties in development, approval, and implementation of models with financial statement impact?
- Are assumptions and limitations for AI models evaluated?
- Are models tested to ensure they are consistent with goals and objectives set forth in the business case?

Validation & Review:

- Has management implemented quantitative evaluation metrics (such as Retrieval-Augmented Generation Assessment (RAGAS)) to assess AI model quality, reliability, and performance?
- Is there documentation of model validation procedures that meet audit evidence standards?

While AI applications rely on new and evolving technology, the core concepts behind governance, risk, and controls are still pertinent for promoting trust and transparency.

The elements of trust and transparency

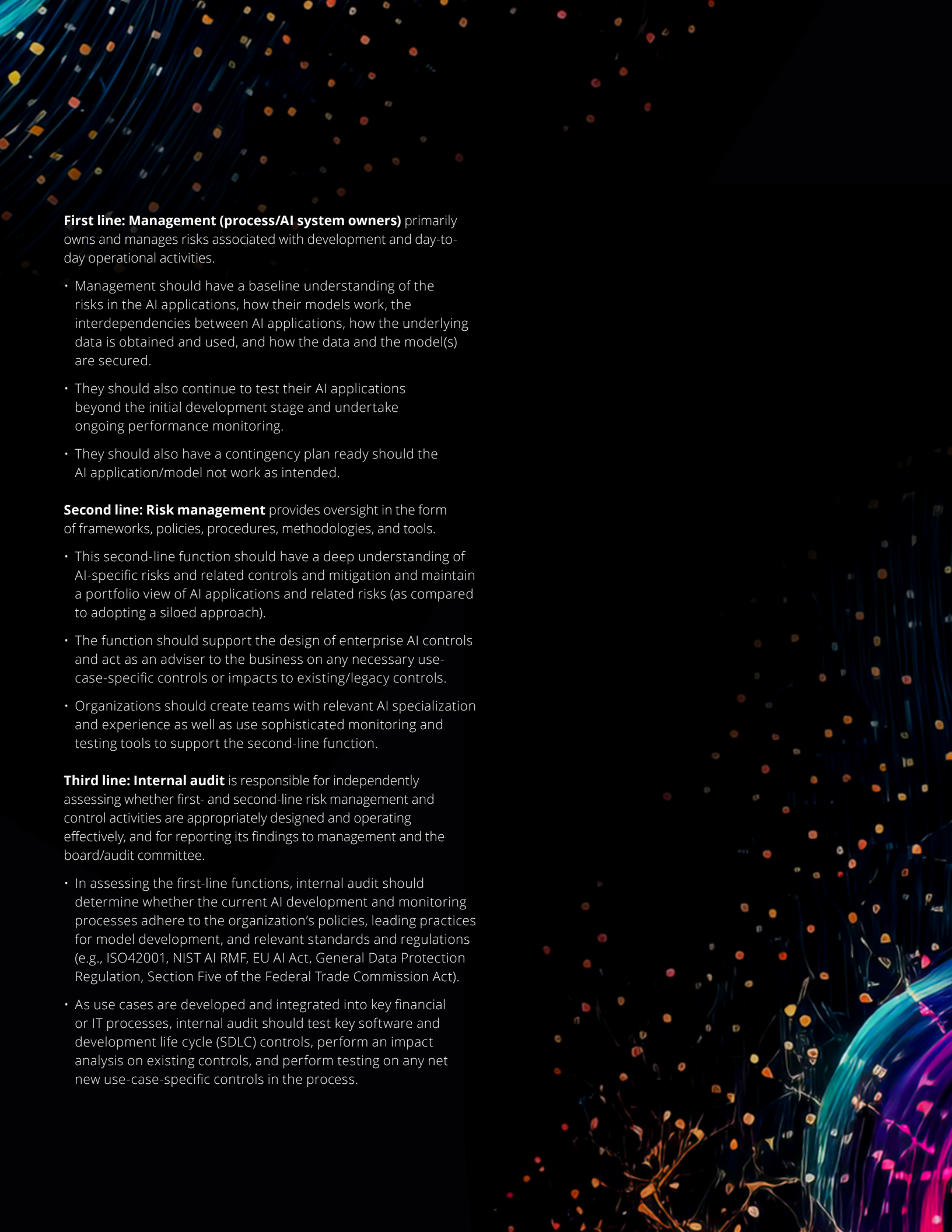
As organizations endeavor to promote trust and transparency, as well as to achieve the organization's goal of accelerating AI adoption, they should adapt existing capabilities along with developing new ones. People, process, data and technology remain key factors for organizations in supporting trust and transparency in the use of AI models.

- **People** – Organizations should leverage existing skill sets (for example, in risk management and controls functions, model risk management). Then they can augment those functions with AI specialists (e.g., model owners, data scientists, and developers). Organizations should also adequately educate employees and board members about AI risks.
- **Process** – It is important to adapt a governance model to include leading practices, relevant frameworks, and regulations that incorporate AI-specific considerations. Organizations should also proactively prepare for risks. Adopting an appropriate framework, such as Trustworthy AI™, can help navigate AI-specific risk considerations like fairness, bias, and explainability.
- **Data** – An AI model can only be as reliable as the data that is inputted into it. Ensuring quality, security, privacy and integrity of data is an absolutely essential aspect of trusted and transparent AI outputs. This becomes particularly important when using third-party AI solutions and data sources. By ensuring good data governance and compliance, the explainability and reliability of AI models can be quickly and directly enhanced.
- **Technology** – Organizations should use cutting-edge tools, including AI and data science platforms, to facilitate controlled processes for model development, deployment and ongoing monitoring of performance. Machine learning operations (MLOps) can help organizations integrate supporting tools and functionality. For example, Omnia's Trustworthy AI module shows how certain tools and functionality can support testing for bias, resilience and reliability, transparency and other dimensions of the Deloitte Trustworthy AI framework.

In an AI environment, A&A professionals can help promote trust and transparency around AI usage in a way that helps mitigate risk in the present and that prepares for the future. With the benefit of an auditor's mindset and risk and controls experience, organizations can source the capabilities they need and that have been there all along—in a trusted and familiar place.

The three lines in terms of AI governance

The questions above illustrate the reasons why organizations need to think broadly about trust and transparency, rather than merely validating the underlying functionality of AI applications. To undertake this broad approach, many organizations across industries have adopted an approach that incorporates essential skillsets, notably quantitative/technical, governance/policy, and internal controls. As AI risks are rapidly evolving, organizations can draw on the existing tools—and professionals—deployed in designing, evaluating and monitoring risks and controls (e.g., model risk, operational risk).



First line: Management (process/AI system owners) primarily owns and manages risks associated with development and day-to-day operational activities.

- Management should have a baseline understanding of the risks in the AI applications, how their models work, the interdependencies between AI applications, how the underlying data is obtained and used, and how the data and the model(s) are secured.
- They should also continue to test their AI applications beyond the initial development stage and undertake ongoing performance monitoring.
- They should also have a contingency plan ready should the AI application/model not work as intended.

Second line: Risk management provides oversight in the form of frameworks, policies, procedures, methodologies, and tools.

- This second-line function should have a deep understanding of AI-specific risks and related controls and mitigation and maintain a portfolio view of AI applications and related risks (as compared to adopting a siloed approach).
- The function should support the design of enterprise AI controls and act as an adviser to the business on any necessary use-case-specific controls or impacts to existing/legacy controls.
- Organizations should create teams with relevant AI specialization and experience as well as use sophisticated monitoring and testing tools to support the second-line function.

Third line: Internal audit is responsible for independently assessing whether first- and second-line risk management and control activities are appropriately designed and operating effectively, and for reporting its findings to management and the board/audit committee.

- In assessing the first-line functions, internal audit should determine whether the current AI development and monitoring processes adhere to the organization's policies, leading practices for model development, and relevant standards and regulations (e.g., ISO42001, NIST AI RMF, EU AI Act, General Data Protection Regulation, Section Five of the Federal Trade Commission Act).
- As use cases are developed and integrated into key financial or IT processes, internal audit should test key software and development life cycle (SDLC) controls, perform an impact analysis on existing controls, and perform testing on any net new use-case-specific controls in the process.

The Deloitte difference

At Deloitte, we believe trust is essential to scaling AI with confidence. It must operate on two levels: the system must be designed to perform reliably, and people must feel secure in using it.

That's why we've built an integrated platform for Trustworthy AI—one that brings together machine-level governance and human-centered design. It's engineered to help organizations develop AI systems that are secure, transparent, explainable, and aligned with intended outcomes.

Backed by Deloitte's AI Institute, supported by global research, and informed by deep experience across industries, this platform helps organizations embed trust into AI development from day one—transforming it from a reactive concern into a proactive capability for responsible growth and long-term value.

Deloitte's Audit & Assurance AI leadership

Deloitte delivers responsible, tested, human-led, AI-powered innovations, addressing complex challenges with practical, trusted solutions. Deloitte's AI-enabled offerings, combined with extensive industry, domain and regulatory experience, can transform financial complexity into strategic clarity. Deloitte's approach is grounded in quality, integrity, and transparency.



Scott Jermy

**AI Assurance Offering Leader
Audit & Assurance Managing Director**
Deloitte & Touche LLP
scjermy@deloitte.com



Ryan Hittner

**Audit & Assurance Principal
AI Assurance**
Deloitte & Touche LLP
rhittner@deloitte.com



Geoffrey Kovesdy

**Digital Controls, Artificial
Intelligence, and Automation
Offering Leader
Audit & Assurance Principal**
Deloitte & Touche LLP
gkovesdy@deloitte.com



Brian Cassidy

**Audit & Assurance Partner
AI Assurance**
Deloitte & Touche LLP
bcassidy@deloitte.com

The services described herein are illustrative in nature and are intended to demonstrate our experience and capabilities in these areas; however, due to independence restrictions that may apply to audit clients (including affiliates) of Deloitte & Touche LLP, we may be unable to provide certain services based on individual facts and circumstances.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2026 Deloitte Development LLC. All rights reserved.