



Artificial Intelligence: IT Audit Considerations with Focus on Information Technology General Controls

Introduction

Artificial intelligence (AI) is increasingly embedded in business and IT processes across industries, including transaction processing, exception handling, forecasting, analytics, and automated approvals. AI is transforming how organizations handle data, make decisions, and report financial information. As AI becomes more integrated into processes that affect financial reporting, it introduces new complexities and risks that auditors, finance leaders, and IT leaders need to understand and address.

Accordingly, an effective IT audit approach starts with a comprehensive understanding of the entity's AI use cases, the related systems and service providers, and the governance and internal control framework surrounding those activities. This understanding is foundational to identifying and assessing risks of material misstatement and designing appropriate audit procedures.



Start with understanding: What is the AI doing, and where does it matter?

Understanding the entity's use of AI involves identifying its purpose, nature, and usage. This includes identifying:

- ▶ The relevant business and/or IT processes where AI is used
- ▶ The activities performed by AI
- ▶ The data provided to the AI
- ▶ The involvement and relevance of third parties (e.g., service providers)
- ▶ Any changes to those processes throughout the engagement period (from planning to completion)

As AI environments can evolve rapidly, the risk assessment needs to remain agile and responsive to changes in data inputs, model updates, and other modifications to the AI solution.



Control activities: What controls should exist over AI-enabled processes?

Entities need both business process controls and IT controls designed and implemented to mitigate associated risks. Risks associated with AI are no exception and, in some cases, may be more complex because AI can generate outputs that appear credible but may be inaccurate. In addition to controls over the AI output and Information Technology General Controls (ITGC), controls should also focus on data inputs, as the quality of AI output depends heavily on the underlying (input) data.

In the 2026 article *Achieving Effective Internal Control Over Generative AI*, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) noted that a key factor in identifying relevant controls over AI solutions is whether AI reliance exists or not. COSO defines “reliance” as a circumstance in which management depends on outputs generated by an AI system in the performance of a control, without sufficiently re-performing or independently validating the underlying activity. A reliance example is when AI automatically matches journal entries to supporting documentation and management approves the posting using only the AI output. A non-reliance example, however, is when AI suggests matches but the control owner re-performs the match and documents the review and approval.

While ITGCs can be relevant in both cases, such controls become significantly more important in reliance use cases.

In evaluating AI-enabled processes, auditors should distinguish between AI-related risk considerations and the ITGC implications of those risks. AI-related risk considerations may include matters such as the quality and completeness of data inputs, the reliability of AI-generated outputs, model updates, or changes in model behavior over time. These considerations also include whether incomplete, unrepresentative, or poor quality data could introduce bias into the model, as well as whether changes in data patterns, business conditions, or model performance over time could result in model drift. ITGC implications, by contrast, relate to whether the relevant technology components supporting the AI-enabled process are subject to appropriate controls over access, change management, operations, and development. Maintaining this distinction helps ensure the audit approach addresses both the process-level risks introduced by AI and the relevant technology controls over the systems and components in scope.

IT General Controls

For AI solutions, the traditional ITGC domains remain relevant, including:

- ▶ User Access
- ▶ Program Change
- ▶ Computer Operations
- ▶ Program Development

The key difference is not that AI requires entirely new ITGC categories but that these controls may need to extend beyond traditional applications, databases and operating systems to additional AI related components in the "AI ecosystem."

AI related components may span both Software as-a Service ("SaaS") solutions and on-premises systems. As a result, relevant ITGCs may be performed by the entity and third-party service providers, depending on how the solution is designed and operated. The specific components in scope can vary by AI use case. These may include the AI model itself that performs the underlying inference, whether a foundation model provided by a large-scale AI service provider or a fine-tuned model tailored to the entity's needs. Relevant components may also include data pipelines used to clean, process, and feed data into the model. Another relevant component may be orchestration software used to manage AI components and execute workflows, such as monitoring transactions and routing data from data pipelines to AI models. Depending on the use case, AI agents may also be relevant components, particularly where they interpret objectives and perform actions with limited human intervention. In addition, enterprise AI platforms may be relevant. These platforms may combine multiple components, such as the model and agents (for example, some enterprise platforms embed multiple AI capabilities across integrated business applications and workflows).

For each component, auditors should perform a risk assessment and scoping exercise to determine which ITGCs are relevant to the audit. This assessment should consider the nature of the component, the degree of reliance placed on it, and whether controls are performed by the entity or by a service provider.

Auditors should also evaluate how the use of AI affects ITGC considerations for existing in-scope systems, including common platforms such as ERP systems, particularly where AI-enabled tools or agents interact with those systems, process data from them, or initiate actions within them. For example, when AI agents have access to the ERP system, one crucial task is to assess whether existing ERP access controls, such as user access reviews, appropriately address the access of the AI agents. To do so, it is important to identify the specific AI component and the related use case, as AI agents may be deployed in different ways which include agents natively delivered within the ERP system; external AI agents interacting through the user interface, or "headless" agents connecting through an application programming interface (API). In each scenario, the auditor should look to identify how the AI agent is addressed within the company's ITGC framework.



In summary, foundational steps when auditing ITGCs in the context of AI involve identifying how the company uses AI, including all relevant AI components, and determining the use case and the level of reliance placed on those components in order to assess ITGC coverage. As organizations continue to expand their use of AI, proactively evaluating these areas can help strengthen governance, reduce risk, and support audit readiness—connect with [BDO's Technology Risk Assurance](#) team to discuss how your organization can align its AI initiatives with a robust ITGC framework.

CONTACT US

TIM STROBEL

Assurance Managing Director Technology Risk Assurance

tstrobel@bdo.com

Have questions or want to learn more? CONTACT US!