Deloitte.

Heads Up | Volume 33, Issue 3
April 3, 2026

In This Issue

COSO Releases Publication on Internal Controls Related to Generative AI

Overview

On February 23, 2026, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released a publication, *Achieving Effective Internal Control Over Generative AI* (the "COSO GenAI guidance"), that builds on COSO's *Internal Control — Integrated Framework* (2013) by introducing a pragmatic approach to managing the new and evolving risks and internal controls related to generative artificial intelligence (GenAI). The publication takes a capability-based view that focuses on what GenAI can do (e.g., data extraction and ingestion; automated transaction processing and reconciliation; workflow orchestration and autonomous task execution; insight generation; AI-powered monitoring and continuous review; human-AI collaboration) and aligns risk identification and control expectations with the 17 principles embedded in the five components, as outlined in the integrated framework.[1]

In addition to its integration with the most commonly used framework for evaluating internal control over financial reporting, a core strength of the COSO GenAI guidance is its implementation roadmap consisting of six steps — govern, inventory, assess, design, implement, and monitor. This roadmap can be readily converted into both a management workplan and a consistent tool for compliance and risk management functions (e.g., internal auditors, information technology risk management, legal), the governance structure (i.e., the board of directors), and external auditors to use in understanding how AI has been implemented at an organization. The COSO GenAI guidance directly addresses significant risks and challenges with GenAI, including rapid change, limited explainability, and uncontrolled adoption ("shadow AI"), emphasizing the need for ongoing inventories of AI use cases throughout an organization, clear ownership and escalation paths, and continuous monitoring of control performance.

[1] For a chart listing the five components and 17 principles, see page 5 of the COSO GenAI guidance.

We believe that the COSO GenAI guidance is most effective when treated as building on the 2013 framework, not as a prescriptive rulebook. GenAI necessitates a fundamental shift in mindset for both management and auditors, moving from deterministic, rule-based technologies to probabilistic models with inherently variable outcomes, and from static, point-in-time assurance to continuous monitoring of model performance and risk. Monitoring plays a key role when GenAI is used in financial reporting, since "set-and-forget" does not work. Effective monitoring prioritizes meaningful evaluation of key performance indicators, including, for example, transaction volume, transaction size, and override percentages, to detect model drift or other performance issues. It is also important to perform evaluations of accuracy and reliability as well as more robust assessment of the root causes of deficiencies (e.g., prompt design, retrieval issues, vendor changes).

Actions to Manage Risk

Looking ahead, organizations can take the following six actions to manage risks and perform effective scaling:

1. Establish cross-functional GenAI governance with defined roles, accountability, controls, and escalation protocols to ensure consistent oversight of all GenAI use cases, including "Shadow AI," throughout the organization and at service organizations.
2. Maintain a GenAI use-case inventory and map in-scope use cases to key business processes, relevant assertions, and key controls (including controls over spreadsheets, tools, upstream data, and system interfaces) to enable consistent oversight and informed decision-making at scale.
3. Apply a use-case-based decision framework to right-size the level of human involvement — including review, approval, and segregation of duties — on the basis of the risk profile of each use case and the degree to which GenAI outputs drive or influence business decisions or automated processes.
4. Implement COSO-aligned control "building blocks" for GenAI across the organization, such as:
    - Access and acceptable-use restrictions (including vendor tools and plugins).
    - Input/data controls and retrieval constraints.
    - Prompt/configuration governance and change control.
    - Output validation and exception handling, including acceptance and accountability for the output.
    - Logging/traceability (model/version, prompts, key inputs/outputs, approvals).
    - Monitoring controls for drift, anomalies, and unauthorized use.
5. Apply heightened rigor to financially relevant GenAI use cases by mapping in-scope use cases to financial reporting processes, relevant assertions, and key controls, and ensure GenAI outputs that could affect material amounts recorded or disclosed in the financial statements, or controls over relevant application systems, journal entries, reconciliations, or estimates (including management review controls), receive appropriate human oversight and are supported by appropriate evidence.
6. Ensure appropriate communication, alignment, and documentation. Early on, management should coordinate with internal and external auditors to determine what constitutes sufficient, appropriate evidence for GenAI-enabled control activities and monitoring.

Implementation of AI governance will require strong understanding of the risks and thoughtful consideration of the details of use-case specific control design. Beyond a strong framework and policy, AI governance ensures that use cases are designed well and operating effectively.

Deloitte's Audit & Assurance AI Leadership

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

Contacts

Michelle Donahue
Audit & Assurance
Managing Director
Deloitte & Touche LLP
+1 201 675 8631
midonahue@deloitte.com

Ryan Hittner
Audit & Assurance
Principal
Deloitte & Touche LLP
+1 646 715 5612
rhittner@deloitte.com

Geoffrey Kovesdy
Audit & Assurance
Principal
Deloitte & Touche LLP
+1 617 462 1386
gkovesdy@deloitte.com

Todd Lindsey
Audit & Assurance
Partner
Deloitte & Touche LLP
+1 561 962 7656
tlindsey@deloitte.com

Amy Steele
Audit & Assurance
Partner
Deloitte & Touche LLP
+1 203 423-4518
asteele@deloitte.com

Dbriefs for Financial Executives

We invite you to participate in Deloitte's live Dbriefs webcasts for valuable insights into important developments affecting your business. The Dbriefs for Financial Executives series covers various accounting, governance, and financial reporting topics. Dbriefs also provide a convenient and flexible way to earn CPE credit — right at your desk.

Subscriptions

To subscribe to Dbriefs, or to receive accounting publications issued by Deloitte's Accounting and Reporting Services Department, please visit My.Deloitte.com.

The Deloitte Accounting Research Tool

The Deloitte Accounting Research Tool (DART) is a comprehensive online library of accounting and financial disclosure literature. It contains material from the FASB, EITF, AICPA, PCAOB, and SEC, in addition to Deloitte's own accounting manuals and other interpretive guidance and publications.

Updated every business day, DART has an intuitive design and powerful search features that enable users to quickly locate information anytime, from any device and any browser. While much of the content on DART is available at no cost, subscribers have access to premium content, such as Deloitte's *FASB Accounting Standards Codification Manual*. DART subscribers and others can also subscribe to *Weekly Accounting Roundup*, which provides links to recent news articles, publications, and other additions to DART. For more information, or to sign up for a free 30-day trial of premium DART content, visit dart.deloitte.com.