

Component 3 Monitoring Update

This agenda item provides the Board with an update on notable developments in the technological landscape relevant to audit and assurance engagements, based on the Technology Team's monitoring activities in accordance with Component 3 of the IAASB Technology Position. **See also Agenda Item 7, Section II, including the Matters for IAASB Consideration.**

The developments outlined in this paper are organized into themes, A) to H), that reflect the most notable and relevant developments observed.

A) AI Governance, Explainability, and Transparency

1. **AI Governance:** As organizations integrate artificial intelligence (AI) into their operations, the attention on robust governance and control mechanisms is increasing. Publications from professional accountancy bodies outline the role of accountants in AI governance, quality management, and AI assurance, covering the evolution of AI, key governance components, and the role of assurance engagements in building trust.
2. **Regulatory oversight:** Audit regulators have noted early-stage adoption of AI in audit tools, with limited examples in public company audits. Publications from regulators have identified areas whereby AI could enhance quality, while introducing new risks associated with these tools. Some oversight strategies include influencing firms on how they design and integrate controls over emerging technologies.
3. **AI model explainability and transparency:** There are concerns about AI decision-making processes operating as "black boxes"—producing outputs in ways that cannot be easily understood or tested by auditors, which affects transparency and the ability to challenge evidence. Regulators are also debating acceptable thresholds for AI model interpretability in audit, balancing the need for transparency with practical implementation realities.

B) AI Use by Auditors

4. **AI integration in firm audit workflows:** Firms are incorporating AI into various stages of audit workflows, including risk assessment, substantive procedures, and other core audit tasks. Examples include generative AI being used to draft working papers, analyze complex datasets, simulate audit scenarios, and identify anomalies or trends. Adoption has been aimed at enhancing efficiency, improving coverage and insight, and enabling more dynamic, data-driven audit procedures.
5. **Auditor-led AI innovation and agent-based tools:** Some auditors are experimenting with AI agents to improve task automation and knowledge retrieval. Regulators and other observers have also noted the prospect of autonomous AI agents undertaking more complex audit work in the future, potentially reshaping parts of the audit cycle and resource allocation.
6. **AI-generated evidence and assurance considerations:** AI systems are generating audit evidence in a growing number of engagements, with examples ranging from automated transaction matching to anomaly detection reports used as part of substantive testing. This expansion has prompted questions on the reliability and sufficiency of such evidence, particularly when underlying algorithms are opaque or rely on third-party data sources. It also raises issues about how auditors document

and corroborate AI-generated outputs in compliance with existing requirements, and whether additional procedures or professional judgment frameworks are needed to assess their appropriateness.

C) AI Use by Audited Entities

7. **AI use by audited entities and evolving audit procedures:** Monitoring noted growth in AI adoption across client entities, prompting auditors to assess data integrity, operational controls, governance maturity, and risk management practices. In many cases, this involves evaluating AI-driven processes embedded in core operations and considering the sufficiency of governance frameworks, alongside the development of tailored audit procedures. These include testing the design and operating effectiveness of relevant controls, assessing the appropriateness of data inputs, evaluating the integrity and transparency of AI model outputs, and understanding how such processes integrate with broader business workflows. In some cases, auditors are involving IT specialists to evaluate algorithms, model training data, and bias mitigation measures, and are developing strategies for documenting findings in a manner consistent with audit evidence requirements.

D) Emerging AI Risks and Disruptive Potential

8. **Risk associated with intersection of Quantum Computing, AI, and Agentic AI:** The convergence of these technologies introduces novel risks, with quantum computing in particular posing potential threats to current encryption methods, secure data transmission, and blockchain integrity. Combined with AI and agentic AI, these developments could create complex vulnerabilities in data integrity, algorithmic reliability, and the resilience of assurance systems.
9. **Evolving concepts of “AI Assurance” and applicability of SOC engagements:** There have been varied and sometimes conflicting interpretations of the term “AI Assurance,” with no consistent definition or agreed scope across jurisdictions and stakeholders. Discussions included whether existing frameworks for service organization control (SOC) engagements could be adapted to cover AI systems and processes, and what additional considerations might be needed to address AI-specific risks. This uncertainty creates differing expectations among stakeholders and could influence how assurance services develop in response to AI adoption.
10. **Potential for significant disruption of the profession:** AI and related technologies could fundamentally alter audit roles, workflows, and the market for assurance services. This disruption may include shifts in the types of skills auditors require, increased automation of traditionally human-led procedures, changes in firm structures and service offerings, and potential redefinition of the scope and value proposition of assurance in a technology-driven environment.
11. **Standard-setting cadence:** The speed of technological change risks outpacing the ability of standard-setting processes to adapt, potentially creating gaps in applicability. This may lead to periods where emerging technologies are widely used in practice before relevant guidance exists, creating uncertainty for practitioners and external stakeholders.

E) Data Analytics and Alternative Information Sources

12. **Data Analytics:** Expansion of data-driven audit approaches is continuing, including automated analytical procedures and integration with other technologies to support risk assessment and substantive testing. Continued uncertainty over the use of data analytics for multiple purposes (risk

assessment and substantive testing) has been identified.

13. **Use of non-financial data:** Auditors are leveraging a growing range of alternative technology-driven data sources—including drone and surveillance images, IoT sensor and voice data—to obtain audit evidence such as the operating status of machines. Emerging possibilities include satellite-based optical and radar imagery to assess conditions or confirm the existence of property, though challenges with resolution, shooting frequency, and cost remain.

F) Digital Assets

14. **Digital assets and stablecoins:** There have been ongoing developments in digital assets, including stablecoins, and their relevance to audit and assurance engagements. Recent legislation has begun providing emerging frameworks for stablecoins, though practical implications for audit and assurance remain uncertain. These frameworks have provided avenues for practitioners to engage in assurance engagements over the validity of issued stablecoins.

G) Cybersecurity

15. **Cyber Security:** Cyber risks remain a significant concern, affecting client operations, the integrity of audit evidence, and the resilience of technology systems relied upon during engagements. These threats evolve in scale and sophistication, with implications for how auditors assess IT controls, evaluate incident response capabilities, and consider the potential for cyber incidents to disrupt audit processes or compromise evidence.

H) Third-Party Dependencies

16. **Increasing diversity of technology providers and audit firm reliance:** Audit firms, including many SMPs, are engaging with a growing range of technology providers, from established cloud platforms to emerging FinTech and niche audit-tech developers. This has expanded the options available to firms but also heightened the complexity of vendor management, increased dependency risks, and has the potential to constrain technology governance where key services are outsourced.
17. **Audited entities reliance on technology:** Audited entities are increasingly dependent on cloud services, accounting and ERP platforms, and other technology providers, while AI providers are a growing component within their businesses. This reliance is adding complexity in evaluating internal controls, understanding the use of emerging technologies embedded in processes, and determining the scope and sufficiency of third-party assurance reports.