Responsible AI and audits

Are you ready?

Contents

Do you remember your business before AI?

While it hasn't been long, everything already feels different.

From finance and internal audit to IT and R&D, AI is helping teams move faster and think bigger. And you're not alone. Your customers, your service providers and the teams that evaluate your controls and compliance – they're all evolving too.

So, what does the growing use of AI mean for assurance?

CFOs are asking how it impacts internal control over financial reporting (ICFR).

Audit committees want to know whether their oversight is keeping pace. Internal audit teams want clarity on what new data, documentation or evidence auditors may expect when AI touches key processes.
It can feel complex, especially with limited standards to follow. But one principle is straightforward: if AI supports or impacts a process; it will be relevant for the audit.

Auditors and Responsible AI

While you don't need to slow down innovation to prepare for audit attention, you do need to prioritise Responsible AI practices.

Whether AI is supporting decision-making, customer interactions or internal operations, your organisation should be prepared to explain how it's being used, why it is appropriate, and show how it's governed, documented and controlled. These elements are critical for building trust with auditors and stakeholders.

Auditors typically start with a top-down view. They look at the policies, procedures and frameworks that define how AI risks are managed and overseen. That may include how emerging risks are flagged, how risk appetite is set, and how exceptions are handled. They will also examine roles and responsibilities – who is accountable for AI decisions, monitoring and escalation. Most of this is documented through a risk and control framework or structured governance approach.

Auditors will expect evidence that key controls are operating. For example, if your framework requires a model risk review before deployment, they won't just check whether that policy exists. They will look for proof that it happened. That could include reviewer comments, approval sign-offs, bias testing records, issue logs or documentation from explainability reviews. AI governance often introduces new oversight activities and if they're defined in your programme, auditors will expect evidence showing they actually take place.

Your strategies for being audit-ready

Wherever you are in your AI journey, you can build audit-ready practices by focusing on a few core areas:

Establish strong governance

Governance should clearly set out how AI decisions are made, from selecting tools and models to monitoring them over time. It should address explainability, data lineage and documentation, especially when outputs influence financial reporting or regulatory disclosures. Internal audit can provide valuable challenge by reviewing emerging risks and assessing whether controls and governance are operating as intended.

Integrate AI risk into existing risk management

AI risk should be integrated into your existing risk taxonomy and risk and control self-assessments (RCSAs). Doing this shows auditors that AI's unique risk profile is understood, tracked and mitigated through established structures rather than handled in isolation.

Upskill and align your teams

Audit readiness relies on people in the organisation being able to explain how AI is used, governed and validated and why its outputs can be trusted. Process owners and control operators may need context and training to speak confidently during audits, especially if AI is supporting steps previously performed manually.

Build an inventory of AI use cases

By building a complete, accurate inventory of AI use cases linked to core processes and highlighting those with financial internal controls or regulatory relevance, your organisation ensures visibility of AI. This shouldn't rely solely on self-reporting; it should also capture shadow AI, embedded third-party features and unsanctioned deployments. A well-structured inventory creates visibility, supports risk assessment and avoids surprises during audits.

Apply a risk-based approach

Not all AI is equal. Create a classification framework to help prioritise where assurance needs to go deeper. Tagging use cases with factors like business function, regulatory context, internal control relevance and data sensitivity makes it easier to focus on what matters most as AI usage scales.

Validate AI outputs

Every use case should demonstrate how outputs are checked. For financial reporting, this includes documented reviews, exception logs, validation steps, human oversight and fallback procedures. Because AI outputs are often probabilistic, auditors will focus on how you detect errors, manage hallucination risks and monitor ongoing performance.

Preparing for financial audit compliance

Addressing internal controls regarding AI is first and foremost imperative for organisations to manage business and financial risk.

Auditors will anticipate that your AI governance framework includes internal controls that address specific AI risks. This is crucial for all Swiss companies relying on Internal Control Frameworks, especially those regulated by SEC / SOx, and FINMA.

Consider how confident you are in your ability to do the following:

Clearly explain where and how AI is usedin financial reporting

Auditors may ask about AI usage during the audit. Any AI used in journey entry automation, estimates, the close process or other financial reporting relevant activities should be clearly identified in your AI inventory and reflected in your IC programme.

Demonstrate how AI outputs are validated

Be prepared to show how management has gained confidence in AI-generated results / results generated with the support of AI that feed into financial statements and regulatory disclosures – including data integrity checks, review steps and exception handling protocols.

Test the design and effectiveness of controls involving AI

If AI performs or supports a control, document how the control is designed, how it operates consistently and how management tests it. You should also be able to outline how the underlying AI system was developed, deployed, tested and monitored. Risk and Control Matrices (RCMs) may need updating to reflect where AI generates outputs, supports control activities, what AI risk monitoring controls are in place, or which “human in the loop” controls are relevant.

Prepare complete and accurate Internal Controls documentation

Ensure RCMs, narratives and flowcharts reflect AI usage where applicable. Missing or outdated documentation can create misalignment with auditors and introduce avoidable challenges during the audit.

Equip process owners

Those overseeing key financial reporting processes should be able to explain how AI is used, what risks it introduces and how those risks are mitigated through updated controls and governance.

Moving from audit readiness to confidence

True readiness means having governance, documentation and controls that build trust with auditors and stake-holders – not just during year-end, but through-out the lifecycle of AI.

Whether AI is used for automation, forecasting or embedded within third-party tools, your organisation should be able to explain its usage, risk management and related internal controls clearly and confidently during an audit. True readiness means having governance, documentation and controls that build trust with auditors and stakeholders -not just during year-end, but throughout the lifecycle of AI.

Audit readiness is not a one-time exercise. As AI capabilities evolve, expectations for governance and assurance will continue to grow. By establishing strong oversight structures, transparent inventories and robust governance processes today, your organisation will be prepared to answer tough questions with confidence and provide clear, evidence-based narratives on how AI risks are management and how AI is used responsibly and effectively across the business.

Contact us to learn more

Yan Borboën
PwC Partner
yan.borboen@pwc.ch

Mark Meuldijk
PwC Director
mark.meuldijk@pwc.ch

Morgan Badoud
PwC Director
morgan.badoud@pwc.ch

About PwC

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 364,000 people in 136 countries and 137 territories. Across audit and assurance, tax and legal, deals and consulting, we help clients build, accelerate, and sustain momentum. Find out more at www.pwc.com.