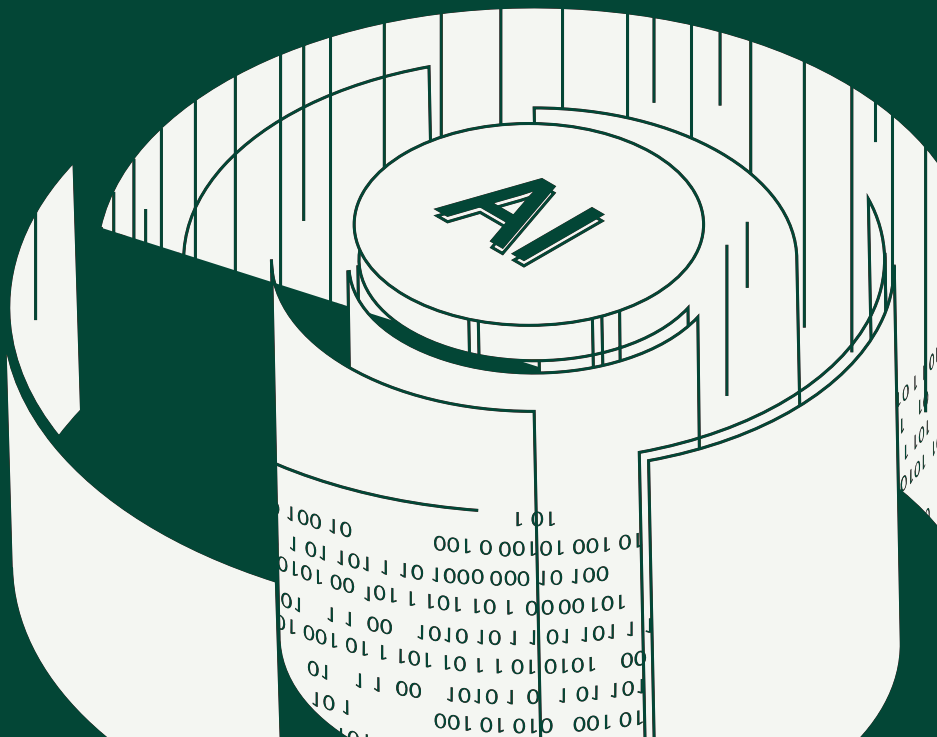
TRULLION

eBook

The 6 Criteria for Evaluating Internal Audit Platforms in the Age of AI

How to Move from Fragmented Workflows to Auditable Intelligence



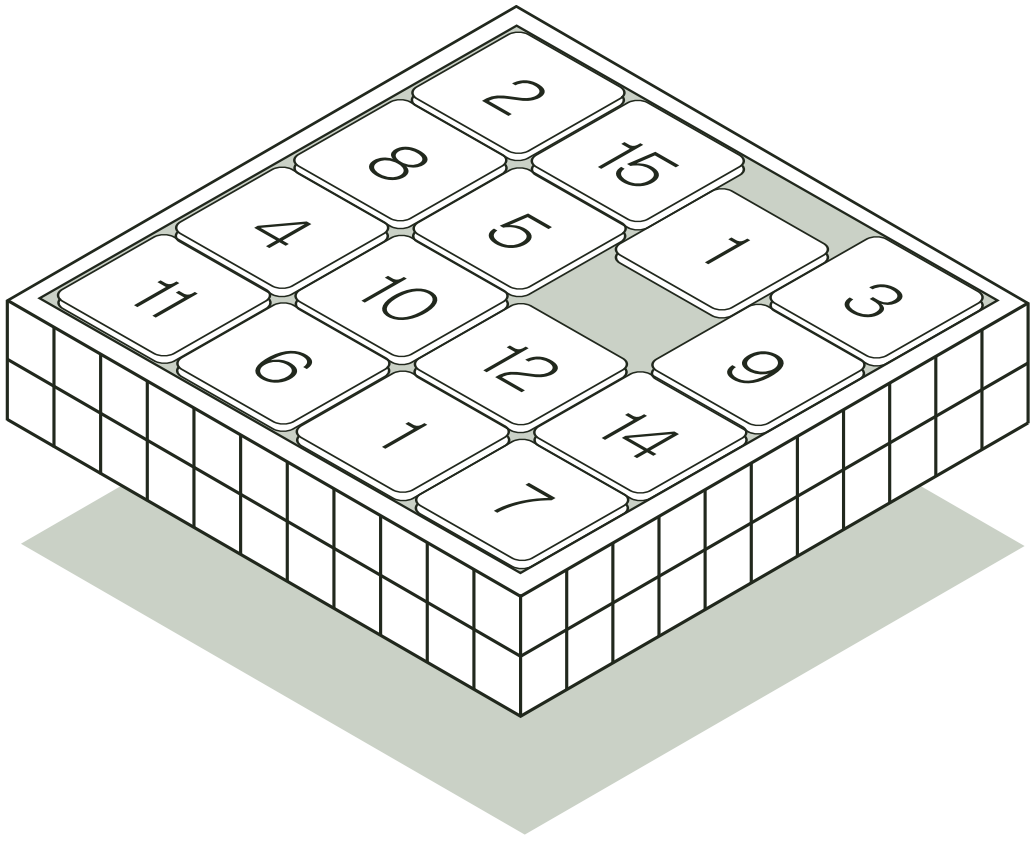
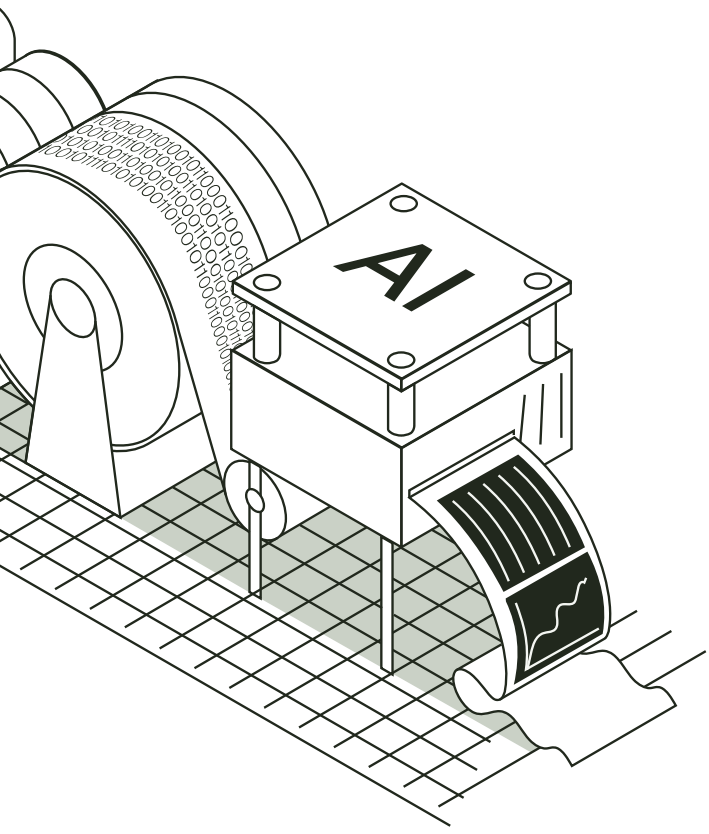


Table of Contents



Introduction: Internal Audit Is Being Asked to Do More With Less

Internal audit is no longer a backward-looking function.

Today's teams are expected to provide assurance across an expanding set of risks, from financial reporting and regulatory compliance to cybersecurity, ESG, and AI governance. Stakeholders want faster insights, greater transparency, and higher confidence in audit outcomes. The IIA's 2024 Global Internal Audit Standards, which became mandatory in January 2025, have raised the bar further, introducing new requirements for strategic alignment, performance measurement, and continuous improvement.

Yet, the resources available to meet these expectations are shrinking.

19%

of internal audit functions reported budget cuts in 2025, up from 11% the prior year (2026 IIA Pulse of Internal Audit)

18%

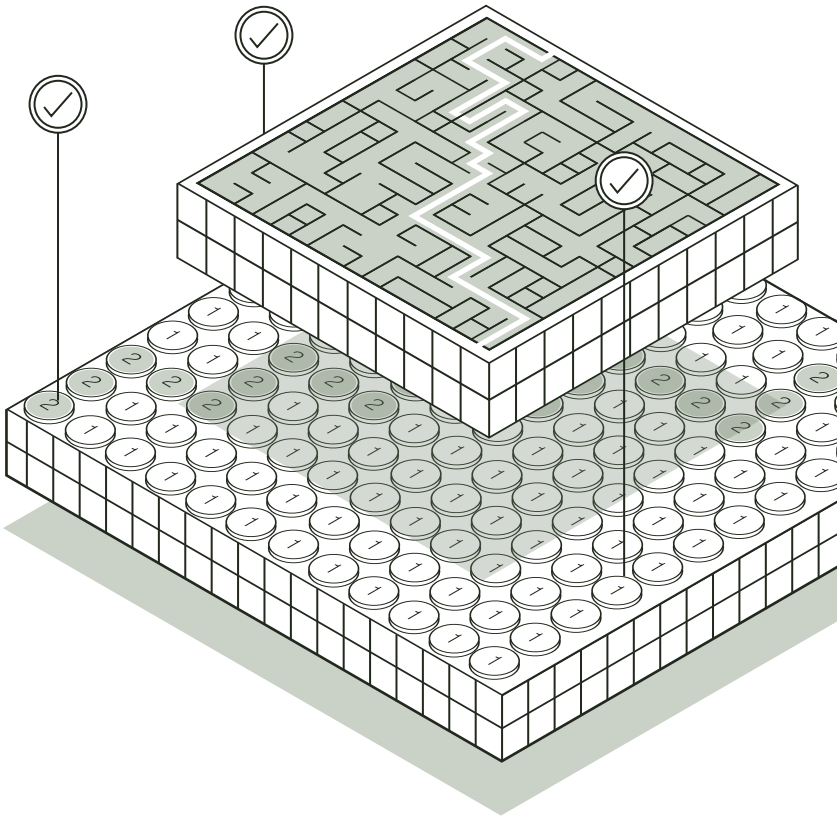
reported staff reductions, the highest level since the 2008 financial crisis (2026 IIA Pulse of Internal Audit)

39%

of internal auditors are currently using AI, with another 41% planning to adopt by end of 2026 (Wolters Kluwer, 2025)

While the scope of internal audit has evolved, the underlying infrastructure has not. Many teams still rely on Excel-based workflows, manual data aggregation, and disconnected point solutions. The result is a widening gap between what audit teams are expected to deliver and what their tools actually enable.

Internal audit hasn't failed to evolve. The systems it relies on have.



The Problem Isn't AI Adoption. It's What Comes After.

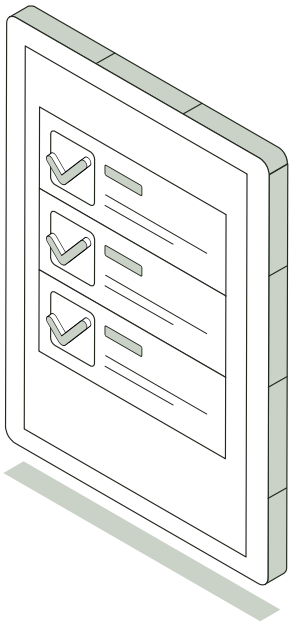
From anomaly detection platforms to agentic AI tools that promise continuous monitoring, the market is moving fast. On the surface, these tools appear to solve many of audit's most persistent challenges. But in practice, many introduce a new set of problems:

- **Outputs without traceability.** AI generates conclusions, but auditors can't trace them back to specific source data or explain how they were reached.
- **Tools outside core workflows.** New platforms sit alongside, not inside, the engagement ecosystem, creating yet another system to manage.
- **Anomaly detection without substantive testing**. Flagging outliers is not the same as deterministic verification against source documents. Many AI tools identify what looks unusual; few can confirm what is actually correct.

The result? More output, but not necessarily more confidence.

AI that can't be audited introduces new risk into a function designed to reduce it.

The goal isn't simply to adopt AI. It's to adopt AI that is reliable, connected, and auditable, AI that strengthens conclusions rather than requiring auditors to validate the technology itself.



What Modern Internal Audit Actually Requires

The 2024 Global Internal Audit Standards introduced a new emphasis on technology. Standard 10.3 requires the Chief Audit Executive to ensure the internal audit function has technology to support the audit process, and to regularly evaluate that technology for opportunities to improve effectiveness and efficiency. This isn't aspirational guidance. It's a mandatory requirement.

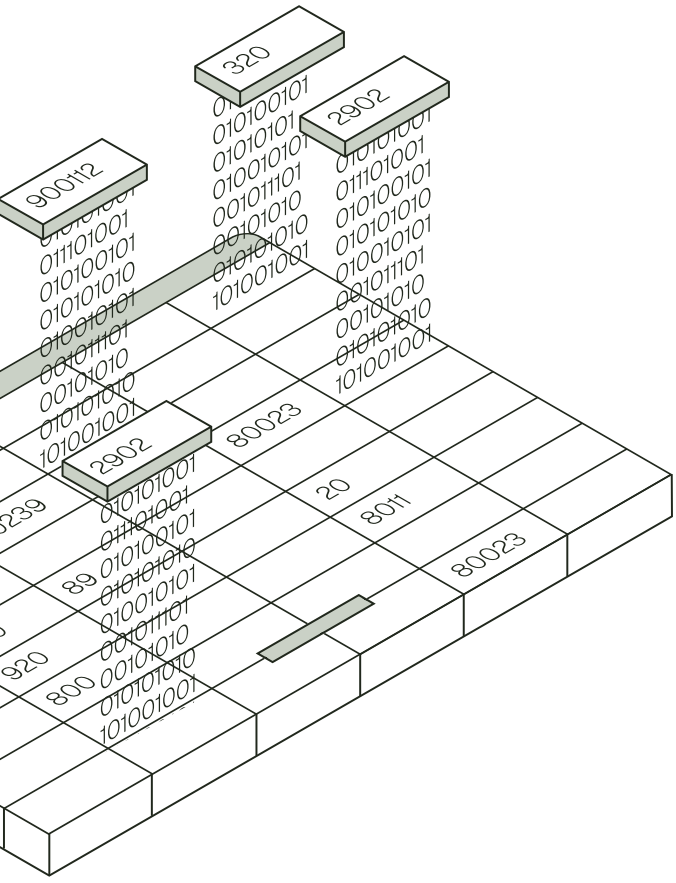
Against this backdrop, three shifts are defining modern audit functions:

From Siloed Data → Connected Data
Audit data no longer lives in one place. It spans ERPs, subledgers, and operational systems. Without connectivity, teams are forced into manual workarounds that consume time and introduce risk. The 2026 Pulse survey found that SOX-compliant organizations devote roughly 30% of their audit plan to financial reporting, yet much of that time is still spent on data collection and preparation rather than analysis.

From Sampling → Full-Population Testing
Sampling was a practical necessity, not a best practice. Modern platforms make it possible to test entire populations, improving both accuracy and coverage. AI tools now enable auditors to test every single transaction in a dataset against control logic, providing deterministic rather than statistical assurance.

From Opaque Automation → Auditable AI
Automation without transparency creates risk. Every output must be explainable, traceable, and defensible. The new IIA Standards reinforce this: they require that evidence be sufficient and appropriate, and that the logic connecting inputs to conclusions be documented and reviewable.

Together, these shifts redefine what an "effective audit" looks like.



The 6 Criteria for Evaluating Internal Audit Platforms

Not all solutions are built for this new reality. The market now includes GRC platforms, anomaly detection engines, Excel augmentation tools, engagement management systems, and generic AI assistants, each solving a piece of the problem, but none addressing it completely.

The following six criteria provide a practical framework for evaluating whether a platform can truly support modern internal audit, not just automate isolated tasks, but transform how audit evidence is created, tested, and defended.

1

Audit-Specific Intelligence
Purpose-built for audit workflows, not repurposed general AI.

2

A Connected Data Foundation
Brings unstructured documents and data into one platform

3

Full-Population Testing
Tests entire datasets, not samples, eliminating projection risk.

4

Auditable AI
Every output traceable, every inference grounded, every conclusion defensible.

5

Unified Workflow and Evidence Management
End-to-end support from planning through reporting, in one system.

6

Enterprise-Grade Trust and Governance
Security, audit trails and access controls that meet standards

1

Audit-Specific Intelligence

Purpose-built for audit workflows, not repurposed general AI.

Internal audit has a distinct logic. It operates under the IIA's Global Internal Audit Standards and produces evidence that must withstand scrutiny from audit committees, regulators, and external reviewers. The way auditors assess risk, document conclusions, and follow audit trails is not simply "data analysis with compliance language added."

The market is now crowded with AI tools that can surface anomalies, flag outliers, or generate risk scores. These capabilities have value, but they are not audit procedures. Anomaly detection identifies what looks unusual; audit testing verifies what is actually correct against source documents, accounting standards, and control criteria. A platform that conflates the two will produce outputs that auditors cannot defend.

General-purpose AI tools, analytics platforms, and even ERP-native reporting modules, were not designed with audit evidence requirements in mind. They can assist auditors, but they don't understand what audit evidence actually requires.

> "Reduced manual audit task time by up to 50% through automated testing across full datasets."
>
> – Tanner LLC

Here's what to look for:

- **Solutions purpose-built for audit workflows.** AI should be embedded directly into audit processes, control testing, reconciliations, walkthroughs, not layered on top as a generic assistant or standalone analytics dashboard.
- **Deep understanding of accounting and financial data.** The system should recognize structures like journal entries, contracts, and disclosures and apply audit logic, not just pattern recognition or statistical scoring.
- **Outputs aligned with audit standards and methodologies.** The platform is built around IIA Standards for documentation and evidence, meaning those standards were part of its design from the start and not something added later.

Generic AI can assist. Purpose-built AI can be relied on.

2

A Connected Data Foundation

Audit evidence doesn't start in a spreadsheet. It starts in source documents.

Most internal audit platforms focus on structured data: GL extracts, trial balances, and transaction registers. These are necessary, but they are not where audit evidence begins. Audit evidence begins in source documents, signed contracts, vendor invoices, board minutes, policy documents, bank confirmations, and lease agreements.

The manual work that consumes the most audit hours is the gap between what those source documents say and what the accounting records reflect. An auditor reads a contract, extracts the relevant terms, finds the corresponding GL entries, and verifies agreement, one transaction at a time. This is the audit trail in its most fundamental form, and most platforms don't touch it.

Many tools in the market today solve only one side of this equation. Analytics platforms ingest structured data and score transactions for risk. Document annotation tools help auditors mark up PDFs. But neither solution bridges the gap between unstructured source documents and structured accounting data.

> "Up to 80% of audit workpapers completed instantly after data upload, eliminating manual prep and data aggregation."
>
> – GRF CPAs & Advisors

A genuinely connected audit platform closes this gap. It works with both unstructured source documents and structured accounting data, and it bridges the two, not just within one document type, but across chains of documents that reference each other.

Here's what to look for:

- **Direct integrations across ERP systems and data sources.** Data should flow automatically from systems like NetSuite, SAP, or QuickBooks, without manual exports or file stitching.
- **Automated data ingestion and normalization.** Raw data should be transformed into audit-ready formats, standardized across sources, and continuously updated.
- **A unified view across structured and unstructured data.** All transactions, documents, and supporting evidence should be accessible in one place, linked, searchable, and ready for testing.

You can't automate what isn't connected.

3

Full-Population Testing Capabilities

Sampling was a constraint, not a choice.

Sampling is not a best practice, it's a constraint the profession has lived with for decades. When audit teams test a sample of transactions, they incur the risk that the sample doesn't represent the population and the burden of projecting findings to transactions they didn't actually examine.

The IIA's updated Global Standards are increasingly explicit about the expectation of rigorous, evidence-backed conclusions, and sampling risk is directly at odds with that expectation.

Modern platforms can test entire populations. This isn't just about efficiency, it changes the nature of what an audit can conclude. When every transaction has been tested, the coverage question disappears. Exceptions become the object of investigation rather than a projection problem. Audit teams can move from "we tested a sample and found no issues" to "we tested the population, and these are the exceptions."

This distinction matters especially in high-risk areas. Revenue, AP, payroll, and access control reviews are all areas where audit committees expect robust coverage. Full-population testing in these areas isn't a nice-to-have, it's a fundamentally stronger audit response.

> Replaced manual sampling with automated, full-population testing, increasing coverage without added effort.
>
> - Tanner LLC

Here's what to look for:

- **Ability to test entire datasets, not just samples.** The platform should automatically evaluate every transaction, control, or record, without requiring manual selection or statistical sampling design.
- **Deterministic matching, not just anomaly scoring.** There is an important difference between flagging outliers and verifying every record against source evidence. The strongest platforms do the latter.
- **Automated, repeatable testing workflows.** Tests should run consistently across periods and entities, reducing variability and improving audit quality.
- **Coverage transparency.** The platform should show exactly what was tested, what matched, and what didn't, with structured guidance for reviewing exceptions.

4

Auditable AI

If the AI can't be audited, neither can the outcome.

This is the most important criterion in the current environment, and the one most often glossed over in vendor conversations.

Internal audit's core function is to provide assurance. That assurance depends on the credibility of the evidence underlying it. When AI generates an output, a conclusion, a match result, a risk flag, the auditor is accountable for that output. If the AI cannot show its work, the auditor cannot defend their conclusion.

"Auditable AI" is not a marketing phrase. It has a specific meaning: every output must trace back to its inputs; every inference must be grounded in identifiable, citable source material; and the logic connecting input to output must be visible and reproducible.

This is where many current market offerings fall short. Tools that use machine learning to score transactions for risk often can't explain why a particular transaction was flagged. Generative AI assistants draft memos and surface research, but their outputs may not be grounded in permissioned, authoritative sources. Agentic AI platforms that automate planning and evidence collection may produce impressive efficiency gains, but if their reasoning can't be inspected and verified, the auditor is left defending a black box.

> Audit procedures that previously took hours now run in minutes, while maintaining full traceability to source data."
>
> – Tanner LLC

Black-box AI models that produce outputs without exposing their reasoning introduce exactly the kind of risk that internal audit exists to manage. **An AI that cannot be audited isn't a solution, it's a liability.**

Here's what to look for:

- **Clear traceability from output back to source data.** Every conclusion, exception, or calculation should link directly to the underlying transaction or document
- **Full audit trail of inputs, transformations, and results.** The system should log how data was processed, what logic was applied, and how outputs were generated.
- **Transparency into how conclusions are generated.** Users should be able to understand, and defend, the reasoning behind results, not just see the outcome.
- **Citation of standards, methodology, or criteria.** Outputs should reference the audit standards or criteria they're grounded in, making review and inspection straightforward.
- **Deterministic execution where it matters.** The most defensible outputs come from rule-based, repeatable processes, not probabilistic models that may produce different results on different runs.

5

Unified Workflow and Evidence Management

Efficiency doesn't come from faster steps. It comes from fewer systems.

Internal audit teams have established workflows, workpaper standards, and engagement platforms that represent years of institutional investment. The most disruptive technology projects in audit have often failed not because the technology was wrong, but because implementation required teams to abandon working systems and rebuild from scratch.

The 2026 IIA Pulse Survey underscores why this matters: SOX-compliant organizations devote roughly 30% of their audit plan to financial reporting and SOX testing. These are high-volume, high-stakes workflows that can't tolerate the disruption of a platform migration. Any new technology must integrate into these existing processes, not replace them.

In practice, this means workpaper-native embedding, where results live inside the templates teams already use, ecosystem integration with engagement platforms, and requiring uniform templates at the outset.

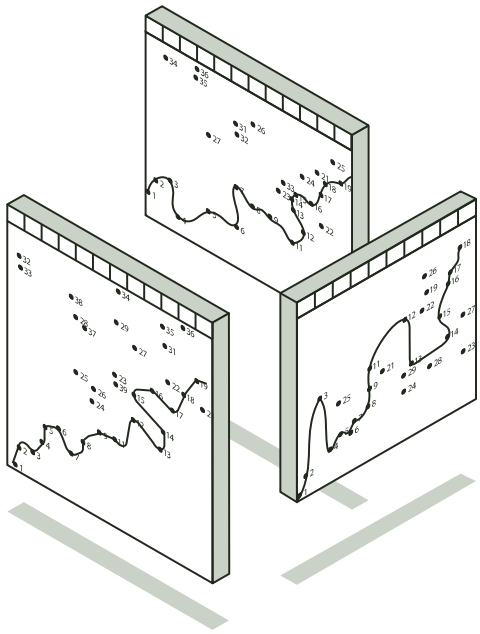
This model also enables incremental adoption. A team that begins with one high-volume audit area, AP reconciliation, payroll, access controls, can standardize that workflow, prove the value, and expand from there.

> Consolidated audit documentation into a single, searchable system, improving efficiency and reducing tool fragmentation across audit teams.
>
> - GRF CPAs & Advisors

This is critical for audit functions operating under budget pressure, where proving ROI quickly is essential to securing continued investment in technology.

Here's what to look for:

- **End-to-end workflow support.** The platform should support the full audit lifecycle, planning, testing, documentation, and reporting, not just isolated steps.
- **Centralized evidence management.** Supporting documents, data, and test results should be stored together, with clear linkage between evidence and conclusions.
- **Workpaper-native execution.** Results should embed directly into existing workpaper formats, not require teams to export from a separate tool and reassemble manually.
- **Ecosystem integration.** The platform should work with existing engagement platforms (Caseware, Thomson Reuters, etc.) and PBC management tools, not force a rip-and-replace.
- **Seamless collaboration across teams.** Teams should be able to review, comment, and iterate within the same system, without versioning issues or tool switching.



6

Enterprise-Grade Trust, Governance, and Control

Trust isn't a feature. It's infrastructure.

Audit functions operate in highly regulated environments where the data they handle is among the most sensitive in any organization. A platform that touches financial records, source documents, and audit evidence must meet the same standards of governance that auditors apply to the systems they evaluate.

This goes beyond checkbox security certifications. The IIA's Global Standards now include explicit requirements around data governance, access controls, and the integrity of audit records. Platforms that support internal audit need to meet these standards not just in marketing materials, but in their actual architecture.

For CAEs evaluating platforms, the question isn't just "is this tool secure?" It's "would I be comfortable if the audit committee asked me to explain how this platform handles our most sensitive data, and could I demonstrate the controls?"

Here's what to look for:

- **Strong security standards.** SOC 2 and compliance with applicable privacy regulations should be baseline requirements, not differentiators.
- **Robust audit logs and version control.** Every action, change, and update should be recorded, ensuring full accountability and reproducibility.
- **Identity and access governance.** SSO, SCIM provisioning, role-based access controls, and automated deprovisioning should be standard. If the platform can't manage its own access controls, it has no place in an audit environment.
- **Workspace retention and locking.** Post-close workspace locking and configurable data retention policies protect engagement integrity and support inspection readiness.
- **Client data isolation.** Multi-tenant platforms must provide logical data isolation between clients, with the architecture to prove it.

Criteria Checklist: AI Platforms for Internal Audit

1 Audit-Specific Intelligence

- Solutions purpose-built for audit workflows
- Deep understanding of accounting and financial data
- Outputs aligned with audit standards and methodologies

2 A Connected Data Foundation

- Direct integrations across ERP systems and data sources
- Automated data ingestion and normalization
- A unified view across structured and unstructured data

3 Full-Population Testing Capabilities

- Ability to test entire datasets, not just samples
- Deterministic matching, not just anomaly scoring
- Automated, repeatable testing workflows
- Coverage transparency

4 Auditable AI

- Clear traceability from output back to source data
- Full audit trail of inputs, transformations, and results
- Transparency into how conclusions are generated
- Citation of standards, methodology, or criteria
- Deterministic execution where it matters

5 Unified Workflow and Evidence Management

- End-to-end workflow support
- Centralized evidence management
- Workpaper-native execution
- Ecosystem integration
- Seamless collaboration across teams

6 Enterprise-Grade Trust, Governance, and Control

- Strong security standards
- Robust audit logs and version control
- Identity and access governance
- Workspace retention and locking
- Client data isolation

Accelerating Internal Audit with Trullion

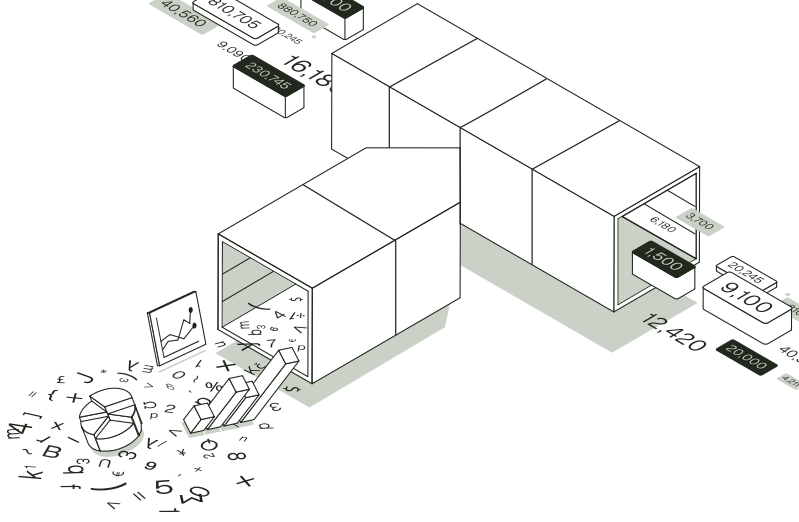
Internal audit is shifting from manual fieldwork and fragmented systems to a more connected, continuous model of assurance. Trullion is built for teams making that transition.

Trullion brings together data, workflows, and audit knowledge into a single platform, designed by former Big Four practitioners and finance leaders who understand the pressures audit teams face.

With Trullion, teams can:

- Automate control testing with data extraction, matching, and exception detection
- Transform raw data into audit-ready datasets, reducing manual prep and accelerating testing
- Validate financial data automatically, including consistency checks, version comparisons, and disclosures
- Centralize policies and audit guidance, embedding standards into every workflow

Critically, Trullion works with existing workpapers and engagement platforms, not as a replacement, but as an execution layer that makes what teams already do faster, more consistent, and more defensible.



GRF CPAs & Advisors

- Reduced audit workflow time by 40% after implementation
- Identified a path to 50–90% total time savings as automation scales
- Workpapers 80% completed instantly after uploading data

Read more

A Foundation Built for Auditable AI

As audit teams adopt AI, one requirement is becoming clear: outputs must be explainable and grounded in source data. Trullion combines deterministic, rule-based execution with citation-backed AI, so every result traces back to its source and every conclusion can stand up to review.

Tanner LLC

- Up to 50% reduction in manual audit effort
- Hours → minutes for key audit procedures
- Hundreds of validations automated annually

Read more

TRULLION

The future of internal audit isn't just automation, it's Auditable AI.

Book a demo at trullion.com

For more information www.trullion.com info@trullion.com