The Role of Artificial Intelligence (AI) in Internal Auditing: Transforming Risk and Compliance

Description

Last updated: 09 October 2026 · Written and reviewed by CA Meet Dhrangadhariya, CSM & Co LLP

Quick summary

- AI is best used for the repetitive, data heavy parts of an internal audit: extraction, matching, full population testing and anomaly flags
- The auditor still owns the scope, the judgment and the conclusion; an AI flag is a lead to examine, not an audit finding
- Key risks are wrong or biased output, poor data quality, confidential data leaving the company and weak documentation of how a result was reached
- Start small: one process, clean data, a written human review step and a record of what the tool did
- Check whether the company is required to have an internal audit under section 138 of the Companies Act, 2013 before planning the scope

A safe way to introduce AI in an internal audit

1. Pick one process with clean, repeatable data

?

2. Define the risk and the test in plain words

?

3. Run the AI tool on the full population

?

4. Auditor reviews every flag and samples what was not flagged

?

5. Document the tool, data, settings and reviewer

?

6. Report findings and agree actions with management

Introduction

Internal auditing has always been about one question: are the company's controls working, and are the risks that matter being managed? What has changed is the volume of data an auditor must look at. A mid sized company can post lakhs of entries in a year, and testing a sample of 25 or 60 of them leaves most of the population unexamined.

Artificial Intelligence (AI) helps close that gap. Tools can read documents, match transactions, score risk and flag anomalies across the whole population. This article explains where AI genuinely helps in an internal audit, where it does not, the risks to control, and a practical way to start.

Where AI helps an internal audit

1. Routine tasks: extraction, matching and reconciliation

Much of audit time goes into collecting and tidying data. AI can:

- Read invoices, receipts, challans and contracts and pull out dates, amounts, GSTINs and terms
- Match bank statements with the books, or purchase orders with invoices and goods receipts
- Check whether an entry follows the company's policy or a standard format

Illustrative example: A manufacturing company has 18,000 bank lines a month. A matching tool pairs most of them automatically and leaves a short list of unmatched or part matched items. The auditor spends time on the exceptions, such as a payment that cleared twice, instead of ticking the matches.

2. Risk assessment and full population testing

Instead of a small random sample, analytics can test every entry against a rule or look for entries that behave differently from the rest. Typical tests:

- Entries posted on holidays, at odd hours or just below an approval limit
- Round amounts, repeated amounts and out of sequence documents
- Vendors with the same bank account or address as an employee
- Sudden changes in a ledger's pattern compared with earlier months

Illustrative example: A finance company ranks its loan accounts by early warning signals such as delayed instalments and frequent restructuring requests. The audit team then picks the highest ranked branches for field work instead of choosing by rotation.

3. Fraud detection

Fraud rarely announces itself; it shows up as small oddities repeated many times. AI can help to:

- Flag duplicate or split invoices

- Spot unusual refund, discount or credit note patterns by location or user
- Compare expense claims with travel, attendance and policy limits

Illustrative example: A retail chain's refund data shows one store with far more refunds than stores of similar size, mostly at closing time and mostly approved by the same user. The flag leads to a review of the bills and CCTV, which is how the actual explanation, genuine or not, is found. The tool pointed to the place; the auditor found the facts.

4. Compliance and regulatory monitoring

AI can help keep checklists current and test them:

- Tracking changes in GST, TDS, labour and company law and mapping them to the company's checklists
- Comparing GSTR-2B with the purchase register and flagging mismatches
- Alerting the team when a due date or a threshold is approaching

Treat the output as a prompt to check the law, not as the law. Tools can be out of date, and a wrong rate or section carried into a report is the auditor's error.

5. Document review with natural language processing (NLP)

NLP lets a tool read long documents and find what matters:

- Missing or unusual clauses in vendor and customer contracts
- Terms that differ from the approved template, such as payment terms or indemnity
- Policy documents that do not match what is actually followed

Illustrative example: An audit team asks a tool to list every vendor contract without a confidentiality or termination clause. The team then reads the short list in full, instead of reading hundreds of contracts to find a few.

What AI does not do

- It does not decide the audit scope or what is material
- It does not understand the business reason behind an unusual entry
- It can give a confident answer that is wrong, and it cannot always explain how it got there
- It cannot take responsibility for the conclusion. That stays with the auditor and the firm

Auditing the AI itself: a growing part of the internal auditor's role

AI is not only a tool for the auditor. Companies now use it in fraud detection, credit scoring, expense approval and customer screening, and internal audit is increasingly asked to give assurance over those systems too. This moves the role from reviewing outcomes to also reviewing the process behind them. A useful review covers:

- **Governance:** who owns the model, who approved it, and who can change it
- **Data inputs:** whether the data is complete, accurate, current and lawfully used
- **Training and validation:** how the model was built and tested, and whether it is re-tested when the business or data changes
- **Bias and fairness:** whether results differ unreasonably across groups, branches or customer types
- **Transparency:** whether the company can explain, in plain words, why the system flagged or rejected an

item
- **Human oversight:** which decisions a person must review, and whether that review actually happens
- **Monitoring and incidents:** logs, error tracking, and what happens when the model is wrong

Internal auditors do not need to build models, but they do need to work with IT, compliance and data teams and to ask for evidence on each of these points.

Risks and the controls to put in place

Risk	What can go wrong	Control
Wrong or invented output	A tool states a figure, section or clause that does not exist	Trace every flag to source documents before reporting
Poor data quality	Duplicate masters, missing fields and wrong mapping give false flags and miss real ones	Clean and reconcile the data first; record completeness checks
Confidential data	Client data sent to a public tool or stored outside India without approval	Use approved tools under a written agreement; remove personal data where possible
Personal data	Employee and customer data processed without a lawful basis	Follow the Digital Personal Data Protection Act, 2023 and the client's data policy
Bias and blind spots	Models trained on past data repeat past patterns	Also test a sample of items the tool did not flag
Weak documentation	Nobody can later explain what the tool did	Keep the tool name and version, settings, data period, output and reviewer in the working papers
Over reliance	Staff stop questioning the result	Define the reviewer's role and sign off every automated test

How to start: a practical approach

1. **Choose one process** with repeatable data, such as bank reconciliation, payables or expense claims
2. **Write the test in plain words** first (for example, "payments to the same bank account under two vendor names") and only then build or buy the tool
3. **Run it on the full population** and also keep a small manual sample to compare
4. **Review every flag** and record the conclusion, including the false alarms; the false alarm rate tells you how useful the test is
5. **Document the work** so a reviewer or another team can repeat it
6. **Agree actions with management** and follow up, like any other internal audit finding
7. **Train the team** on the basics of data, prompts and the limits of the tools before widening the use

Is an internal audit required for your company?

Section 138 of the Companies Act, 2013 read with Rule 13 of the Companies (Accounts) Rules, 2014 requires an internal auditor for listed companies and for prescribed unlisted public and private companies, based on paid up capital, turnover, borrowings and deposits in the preceding financial year. Check the current thresholds for your company, and re-check them every year as the company grows. Even where it is not mandatory, many owners choose an internal audit for control and fraud prevention.

How CSM & Co LLP can help

Our internal audit team can help you:

- Design a risk based internal audit plan and decide where analytics adds value
- Run full population tests on payables, receivables, payroll, expenses and GST data
- Review contracts and policies against your approved templates
- Set up documentation and review steps so that tool based audit work stands up to scrutiny

Please reach out to our team and we will be happy to assist.

Frequently asked questions

Will AI replace internal auditors?

No. AI can read, match and flag very large volumes of data, but scoping the audit, judging whether a flag is a real control failure, talking to management and giving a conclusion remain the auditor’s work. The skill that grows in value is knowing how to question the tool’s output.

Is an internal audit mandatory for every company?

No. Section 138 of the Companies Act, 2013 read with Rule 13 of the Companies (Accounts) Rules, 2014 makes it mandatory for listed companies and for prescribed unlisted public and private companies based on paid up capital, turnover, borrowings and deposits. Please check the current thresholds for your company before deciding scope.

Can an AI flag be reported as an audit finding?

Not by itself. A flag is a lead. The auditor should trace it to the source documents, understand the business reason and confirm the control gap before it goes into a report.

Is it safe to upload company data to a public AI chatbot?

Usually not. Invoices, contracts, payroll and customer data are confidential, and the Digital Personal Data Protection Act, 2023 also applies to personal data. Use tools approved by the client, under a written

agreement, or run them inside the client's own environment.

Do small and mid sized companies benefit from AI in internal audit?

Yes, often for simple things first: matching bank statements to books, finding duplicate invoices, checking expense claims against policy and testing every entry instead of a sample. These need good spreadsheets and clean data more than expensive software.

Official sources

- Institute of Internal Auditors, Global Internal Audit Standards
- Institute of Chartered Accountants of India
- Ministry of Electronics and IT, Digital Personal Data Protection framework

Related reading

- Vibe Coding: How CAs Can Build Tools Without Being Tech Experts

Cited in

This article is cited in the reference list of "The Role of AI in Fraud Detection: Are Financial Institutions Using the Most Effective Systems?" (Hoje Jo, Hien Bui and Damon Moreland), Journal of Finance Issues, Vol. 23, No. 2 (2025). View the journal article.

Disclaimer

This article is for general informational purposes only and should not be considered professional advice. Please consult a qualified expert for advice tailored to your specific situation. The author and website owner are not liable for any errors or actions based on this content.

Date
11/10/2026
Date Created
01/03/2025
Author
meetsoni