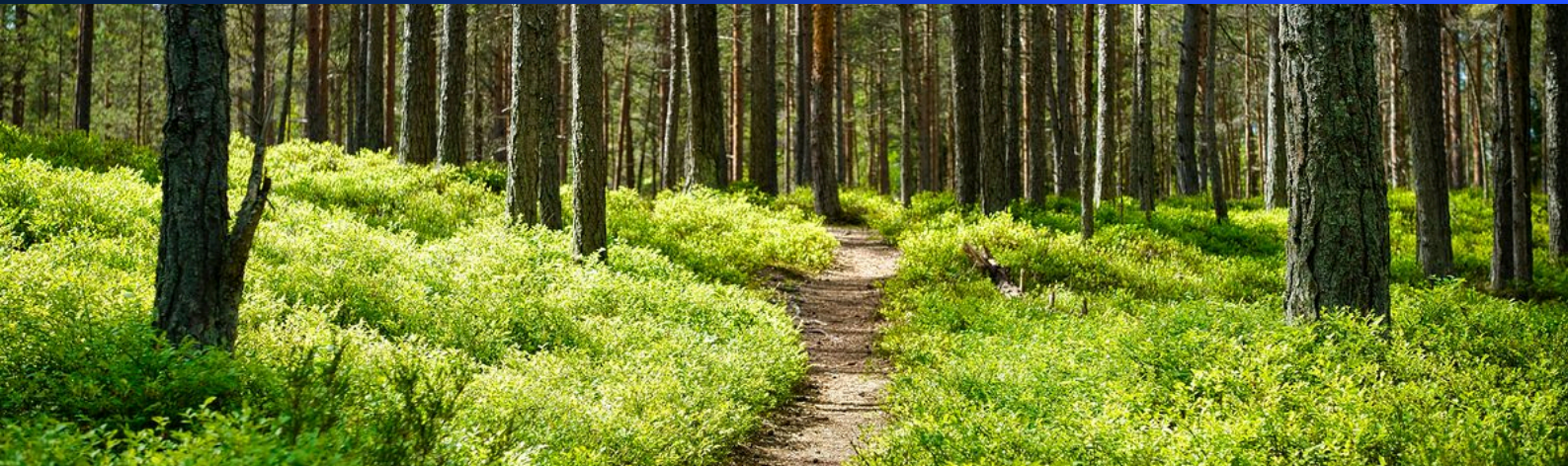


The audit trail requirement is a control, not a software setting

Most companies met the edit-log rule by switching on a feature. Auditors are now asking a harder question: does the trail cover every system and every change, for the whole year?

August 26, 2026 · 10 min read

soniassociates.in/insight-audit-trail-edit-log



AT A GLANCE

- For financial years beginning on or after 1 April 2023, a company that keeps its books in accounting software must use software that records an audit trail of every transaction, logs each change with its date, and cannot be switched off. Auditors now report on it every year.
- Many compliance efforts stopped at the software setting. The requirement goes further. It concerns the books of account wherever they are kept, it has to operate throughout the year, and the trail has to be preserved.
- The recurring gaps sit below the application: direct changes to the database, bulk interfaces, spreadsheets that act as sub-ledgers, and hosted systems where the evidence depends on the provider.
- A defensible position rests on four things: an inventory of systems, control over privileged access, evidence that the feature worked from the first day of the year, and logs kept for as long as the books themselves.

Few provisions in Indian company law have changed audit reporting as much, in as few words, as this one. The requirement is a single proviso in the rules on keeping books of account. It took effect for financial years beginning on or after 1 April 2023, and most companies responded in the obvious way. They asked their software vendor whether the audit trail feature was on, received a reassuring answer, and moved on.

Three reporting cycles later, the conversation with auditors has become more demanding. The question is no longer whether a feature exists. It is whether the trail covers every change to the books, for the whole year, and whether it will still be readable when the law requires it to be produced.

What the rule asks, precisely

The proviso to rule 3(1) of the Companies (Accounts) Rules, 2014 requires every company that uses accounting software for its books to use software that can **record an audit trail of each and every transaction**, creating an edit log of each change made in the books together with the date of the change, and ensuring that the audit trail cannot be disabled.¹

The auditor's side of the obligation is in rule 11(g) of the Companies (Audit and Auditors) Rules, 2014. The auditor reports whether the company used such software, whether the feature **operated throughout the year** for all relevant transactions, whether it was tampered with, and whether the audit trail has been **preserved** as the record-keeping requirements demand.² Books of account must be kept for at least eight years,³ and electronic books must be backed up daily on servers physically located in India.⁴

Read together, three phrases do most of the work: *each and every* transaction, *throughout* the year, and *preserved*. Each of them reaches further than a configuration setting.

Why the software setting is not enough

An edit log inside an application records what users do through that application. It does not necessarily record what happens to the data underneath, or to records kept somewhere else. A typical mid-market company keeps its accounting records across several layers, and coverage varies a great deal between them.

The application layer is usually well covered once the feature is on. The difficulties lie elsewhere, and in almost every company we review they are the same ones.

EXHIBIT 1

Audit trail coverage usually breaks below the application, where the software setting does not reach

Where changes to accounting records happen in a typical mid-market system landscape, and how well each is logged

System layer	What changes there	Typical logging	Coverage
ERP application	Entries, edits, and deletions made through the user interface	Edit log switched on in the software	Covered
Database	Direct updates by administrators or vendor support	Often outside the application's edit log	Gap
Interfaces and uploads	Payroll, bank, point-of-sale, and bulk journal imports	Logged as a batch, not change by change	Partial
Sub-ledgers and spreadsheets	Fixed assets, provisions, credit loss, consolidation	No system audit trail at all	Gap
Hosted and cloud systems	Changes made by the service provider	Evidence depends on the provider's reports	Partial

Illustrative assessment. Coverage depends on the specific systems, configuration, and access controls.

Source: Companies (Accounts) Rules, 2014, proviso to rule 3(1); Companies (Audit and Auditors) Rules, 2014, rule 11(g); SA&A analysis

Soni Aditya & Associates

The four gaps auditors now find

- 1. Database access.** Administrators, and often the vendor's support staff, can write directly to the production database. Changes made there bypass the application and its edit log entirely. Banning database access is rarely practical, because it is sometimes needed. The workable answer is to restrict it to named people, log it at database level, and review privileged activity on a fixed cycle.
- 2. A feature switched on late, or off for a while.** The trail was activated after an upgrade in the second quarter, or disabled during a data migration and turned back on afterwards. Either way it did not operate throughout the year. The evidence that it did, meaning configuration history and system logs showing the feature active from day one, is often not collected until the auditor asks for it.
- 3. Spreadsheets doing the work of sub-ledgers.** Fixed asset registers, provisions, credit loss calculations, and consolidation adjustments are kept in spreadsheets, and only summary entries reach the ledger. Views differ on how far such records fall within the requirement. The safer course is to move material calculations into systems with an audit trail, or to surround them with controls that produce equivalent evidence: locked versions, recorded reviews, and a reconciliation to what was posted.

4. **Hosted systems.** Where accounting or payroll runs on a provider’s platform, evidence of an unbroken trail depends on the provider. Independent service organisation reports covering the full period, together with the controls the company must operate itself, become part of the audit trail position.

An audit trail that covers the application but not the database records the front door and leaves the back door open.

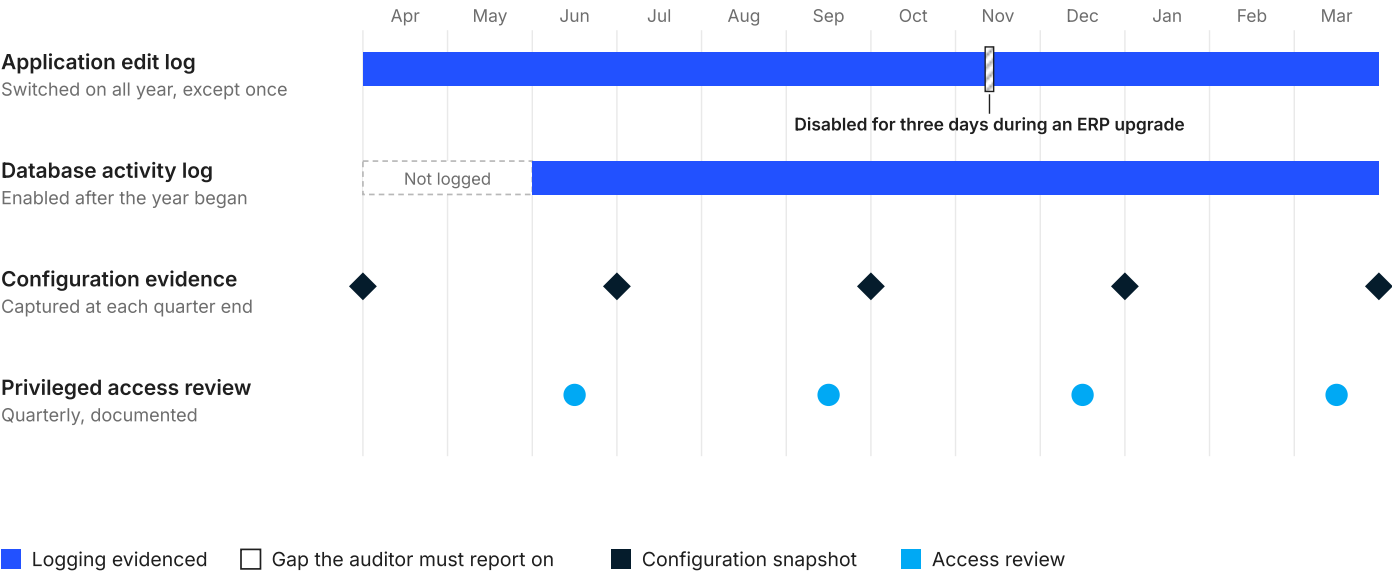
Showing the trail worked for the whole year

The phrase “throughout the year” is where well-intentioned companies most often come unstuck. The evidence has to be gathered as the year goes on, because it cannot be reconstructed afterwards. One weekend of maintenance with the feature disabled creates a gap the auditor has to report, however carefully everything else was done.

EXHIBIT 2

The audit trail has to be shown working for the whole year, and one upgrade weekend can break the record

Illustrative evidence plan for a financial year, including a gap created when the feature was switched off during an upgrade



Illustrative. The auditor reports whether the audit trail feature operated throughout the year for all relevant transactions and whether it was tampered with.
Source: Companies (Audit and Auditors) Rules, 2014, rule 11(g); SA&A analysis

The practical routine is simple. Capture the configuration at the start of the year and at every quarter end. Make any change to audit trail settings subject to formal change control, so that a migration plan has to state how the trail will be kept intact. Review privileged access every quarter, and keep the review signed and dated.

Preservation is the part nobody budgets for

Edit logs grow quickly, and some systems purge them after a retention period chosen for performance. A company that keeps its books for eight years and its edit logs for eighteen months has not preserved its audit trail.

Migration is harder still. A company that moves to a new ERP must still be able to produce the audit trail for the years it spent in the old one. Archiving the legacy database does not help if nobody can read the logs without the software that created them. The retention plan belongs in the migration contract, agreed before it is signed, not after the old licence has lapsed.

FOR AUDIT COMMITTEES

Five questions to ask management

- Which systems create or change our accounting records, and is each one covered?
- Who can change data directly in the database, and who reviews what they did?
- What evidence shows the audit trail worked from the first day of the year to the last?
- Which material calculations still live in spreadsheets, and what controls surround them?
- If we changed systems tomorrow, could we still produce the trail for past years?

Building a defensible position

A position that meets the requirement, and that an auditor can report on without qualification, is put together from a small number of parts:

- **A system inventory** listing every system that creates or changes accounting records, with its audit trail capability, configuration status, and owner.
- **A configuration evidence pack** showing the feature was enabled and unchanged all year, captured at the start of the year and at each quarter end rather than rebuilt at year end.
- **Privileged access controls** over the database and administrator accounts, with logging and a documented periodic review.
- **Interface controls** for bulk uploads and integrations, including file-level logs, control totals, and a reconciliation of what was sent to what was posted.
- **Service organisation reports** for hosted systems, mapped to the controls the company has to run itself.

- **A retention and backup record** showing daily backup in India and logs kept for the full statutory period.

The trail as a forensic record

The audit trail is also the company's own forensic record. When a payment is disputed, when a fraud is suspected, or when a regulator asks who changed a figure and when, the edit log is the one witness that neither forgets nor can be persuaded. Companies that build it properly usually find they have acquired a control they did not set out to build.

NOTES

1. Companies (Accounts) Rules, 2014, proviso to rule 3(1), inserted by the Companies (Accounts) Amendment Rules, 2021, and applicable for financial years beginning on or after 1 April 2023.
2. Companies (Audit and Auditors) Rules, 2014, rule 11(g).
3. Companies Act, 2013, section 128(5).
4. Companies (Accounts) Rules, 2014, rule 3(5), as amended in August 2022.

ABOUT THE AUTHOR

[Aditya Soni](#) is the founding partner of Soni Aditya & Associates and leads its audit, assurance and transaction support work. He is a chartered accountant and was previously in the Assurance practice of Ernst & Young in Pune.

This article reflects the author's understanding of the relevant laws and standards at the date of publication. It is general in nature and is not a substitute for advice on specific facts.

Soni Aditya & Associates, Chartered Accountants, Pune

aditya@soniassociates.in · +91 93400 75288 · [Read online](#)